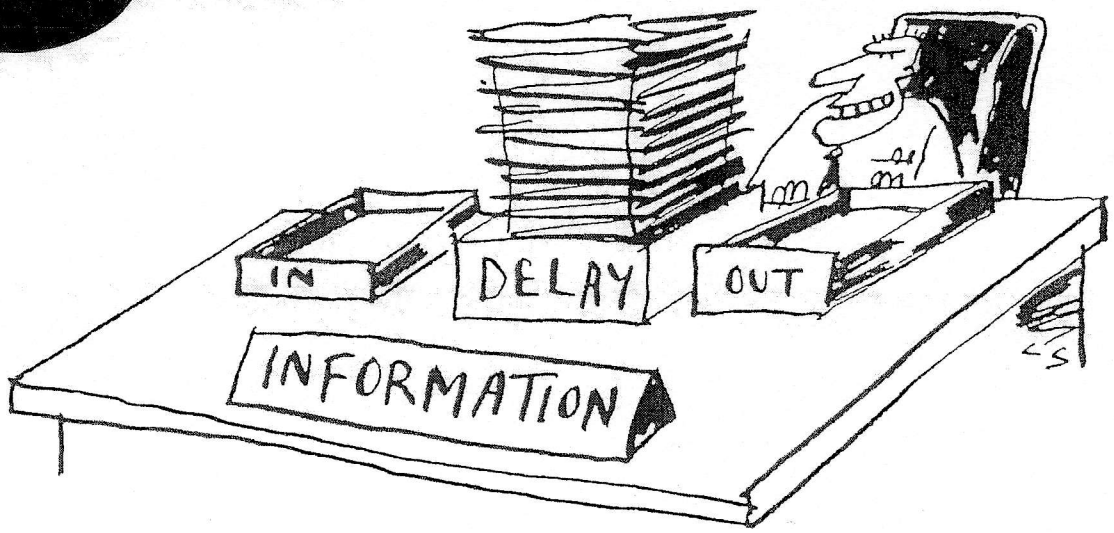
INTERNATIONAL SYMPOSIUM ON FREEDOM OF INFORMATION AND PRIVACY

AUCKLAND,
28 MARCH 2002



Privacy Commissioner
Te Mana Matapono Matatapu

Privacy Commissioner
Te Mana Matapono Matatapu

International Symposium on Freedom of Information and Privacy
Auckland, 28 March 2002

Symposium Papers

Contents

PROGRAMME

8.50 am **Opening Remarks**

Bruce Slane to open the symposium and introduce Grant Liddell as chair for the day.

9.00 **Origins, Background and Scope of Freedom of Information, Personal Access and Data Protection Law: Convergence, Divergence or Parallel Tracks?**

Speaker: Grant Liddell

The typical scope of personal access, data protection and freedom of information laws will be canvassed and set in context as parts of larger schemes of human rights and public accountabilities. Points of similarity and difference, and natural points of tension and divergence, will be highlighted.

9.20 **Interrelationship between FOI and Privacy Laws**

Panel: Bruce Slane, Anand Satyanand, Rick Snell, Chungtong Opassiriwit, John Edwards

An exploration of mechanisms to deal with the interrelationship between privacy and freedom of information laws and, more particularly, to address privacy issues that arise in FOI cases. Panellists briefly outline the processes and highlight their strengths and weaknesses.

- reverse FOI applications in Australia
- consultation between the NZ Ombudsmen and Privacy Commissioner
- combined FOI and data protection review authority
- the purpose of FOI law and the need to effectively protect privacy interests

10.15 Coffee Break

10.35 **Proactive Dissemination of Publicly-held Information**

Panel: David Smith, Bronwyn Keighley-Gerardy, Evelyn Wareham

Transparency and public accountability are promoted by actively disseminating official information. "Routine disclosure/active dissemination" initiatives do not rely on the traditional FOI approach of request and response but on placing documents in physical or electronic reading rooms, promoting best practice in websites, and requiring public bodies to list information and facilitate accessibility.

- Publication schemes in the UK under the new Freedom of Information Act
- Educating and assisting agencies and requesters
- Archives New Zealand Access Standard

11.10 **Dispute Resolution**

Panel: Paul Roth, Chris Puplick, Kevin O'Connor

An exploration of the approaches in two Australasian jurisdictions to reviewing decisions to refuse access for privacy or other reasons under FOI and privacy laws. The models examined include internal-review, Ombudsman-review, and a hybrid model which filters complaints through a commissioner but with recourse to a specialist

tribunal for unresolved cases.

- New Zealand Twins: access review processes for personal and third party requests
- The New South Wales models for review of personal and third party access
- A Judge's perspective on the usefulness of a judicial component in FOI and data protection dispute resolution

12.10 **Special Access Regimes**

Panel: Blair Stewart, Alexander Dix, Jim Tucker, Ulf Brühann

General FOI laws are not the only information access laws in most jurisdictions. There are archives laws, personal access rights in data protection laws, public register laws, court ordered discovery and special regimes covering particular databases or special types of information. This session touches upon some NZ and European examples, including the German approach taken in the extraordinary circumstances posed by the Federal Republic's inheritance of East Germany's secret police files.

- How public register provisions address privacy issues
- The NZ courts' approaches to name suppression
- The Stasi files: How a special access regime balances openness and privacy in relation to secret police files
- Access at the supranational level: the European Union case

1 pm Luncheon

1.50 **Perspectives From Users**

Panel: Nicky Hager, Eugene Bingham

A researcher, author and campaigner, and an experienced journalist, reveal something of their experience of active use of NZ's Official Information Act, noting its strengths and shortcomings.

2.20 **Roundtable Discussion**

Panel: Bruce Slane (session chair), Nigel Waters, Anand Satyanand

A panel discussion with audience Q&A.

3.15 Coffee break

3.25 **The Future**

Panel: Paul Chadwick, Blair Stewart, Tim McBride, Hansjürgen Garstka

This session looks to the future. In what direction is FOI law heading? Will FOI law remain relevant? What direction should law reform go? Does privatisation challenge the traditional rationale of FOI laws? Is there a developing 'globalisation of transparency'? What opportunities exist for sharing experiences on FOI and privacy issues?

4.20 **Closing Remarks**

Brian Pink will offer his personal reflections on the day before Bruce Slane closes the Symposium.

SPEAKERS

Eugene Bingham is a senior journalist with the *New Zealand Herald* who regularly uses the Official Information Act in the course of his work.

Ulf Brühann is a senior official in the Internal Market Directorate of the European Commission, based in Brussels. He is currently adviser responsible for the questions relating to the European Data Protection Supervisor.

Paul Chadwick is the first Privacy Commissioner for the Australian State of Victoria. A journalist and lawyer, he has written books on FOI and media ownership.

Dr Alexander Dix was Deputy Data Protection Commissioner for Berlin before being elected by the Brandenburg legislature as its Data Protection and Access to Information Commissioner in 1998. He became the first Commissioner with a combined remit for privacy and freedom of information in Germany.

John Edwards practices in information law and public policy and is appointed as a District Inspector of Mental Health, having earlier worked for both the Ombudsmen and Privacy Commissioner. He was a member of the Ministerial Working Group on Whistleblowing.

Prof Dr Hansjürgen Garstka is the Data Protection and Information Access Commissioner for Berlin state. His office also serves as the Secretariat of the International Working Group for Data Protection and Telecommunications.

Nicky Hager is an independent researcher and author with degrees in physics and philosophy. In the 1970s and 1980s he was a prominent campaigner and researcher on nuclear, military and environmental issues. His 1999 book *Secret Power: New Zealand's Role in the International Spy Network* caused international controversy and led to a year-long investigation by the European Parliament.

Bronwyn Keighley-Gerardy was appointed in 1993 as Western Australia's first Information Commissioner.

Grant Liddell, Crown Counsel in the Crown Law Office, Wellington, was formerly a law academic at the University of Otago. He co-authored *Freedom of Information in New Zealand.*

Tim McBride has been actively involved in the privacy area in New Zealand for many years as an advocate, author, barrister, commentator, consultant and lecturer. He currently teaches a course in privacy law at the University of Auckland.

Judge Kevin O'Connor is the President of the New South Wales Administrative Decisions Tribunal which receives, amongst other things, appeals under the state's Privacy and Freedom of Information laws. Previously, he was Australia's first Federal Privacy Commissioner.

Chungtong Opassiriwit is the Director of Thailand's Official Information Commission. His office serves as secretariat for both the information commissioners, who are responsible for access complaints, and the Tribunal, which determines disclosure cases.

Brian Pink was appointed Government Statistician and Chief Executive of Statistics New Zealand in October 2000 having formerly worked in the Australian Bureau of Statistics.

Chris Puplick is New South Wales' first Privacy Commissioner, having earlier chaired the state Privacy Committee. He concurrently chairs the NSW Anti-Discrimination Board

Dr Paul Roth Associate Professor of Law at the University of Otago is the author of *Privacy Law & Practice*, New Zealand's principal legal reference work on privacy law.

Judge Anand Satyanand is a judge of the District Court but is currently a full time Ombudsman in which capacity he reviews complaints under the Official Information Act.

Bruce Slane is New Zealand's first Privacy Commissioner. Prior to this Bruce practised as a lawyer, was President of the New Zealand Law Society, and chaired the Broadcasting Tribunal.

David Smith is Assistant Commissioner with the United Kingdom Office of the Information Commissioner.

Rick Snell is a lecturer in law with the University of Tasmania. He edits the *FOI Review* and is a well known Australian authority on freedom of information matters.

Blair Stewart is Assistant Commissioner with the Office of the Privacy Commissioner. He also serves on the editorial panel of *Privacy Law & Policy Reporter* and as a consultant editor to *Human Rights Law and Practice.*

Jim Tucker is Head of Journalism at Western Institute of Technology. A former editor of the *Sunday Star-Times*, he holds a masters degree in media ethics and has produced the basic journalism textbooks used by NZ journalism schools for the past decade.

Evelyn Wareham is Senior Archives Analyst with Archives New Zealand. In 2001 she coordinated the development of Archives New Zealand's Access Standard.

Nigel Waters was Assistant Data Protection Registrar in the UK and Deputy Privacy Commissioner in Australia, before becoming a consultant in fair information practices and privacy. He is based in Sydney and is Associate Editor of *Privacy Law & Policy Reporter.*

INTRODUCTION

Bruce Slane
New Zealand Privacy Commissioner

> *Speech is not free. It costs lives; or its price can be another value we hold dear. I believe that the cost of free speech is usually a price worth paying. Yet so many of those who purport to value free speech betray their ideals by failing to analyse exactly why freedom of expression is important, or from whom threats to free speech arise, or when it is wrong to exercise the right to free speech.*
> - Simon Lee, *The Cost of Free Speech*, 1990

I am pleased to introduce this International Symposium on Freedom of Information and Privacy. While New Zealand has highly regarded laws governing both information privacy and access to information, I cannot recall there ever being a New Zealand conference devoted solely to discussing freedom of information and privacy together.[1]

There has been high public interest in the Symposium. The conference fee was pitched at an affordable level to encourage public participation (although a higher fee and lower participation would have meant less work and more funding for my office!) The 120 person capacity of the original venue proved insufficient. I am honoured to note the international nature of the event. In addition to the majority of speakers being from overseas I can report that no fewer than 16 countries are represented in the audience.[2]

Freedom of Information

The Symposium deliberately uses the phrase "freedom of information" even though the phrase, and the contraction "FOI", are not used much in New Zealand. It has been adopted to encapsulate an expansive concept, and collection of laws, relating to access to information, transparency and "open government". The Official Information Act 1982 (OIA), notwithstanding its misleadingly broad title, is simply the most important of the access to information laws. Two other premier access laws are the Privacy Act 1993, governing access by individuals to information held about themselves, and the Local Government Official Information and Meetings Act 1987 (LGOIMA).[3] LGOIMA is also an example of another species of FOI law: the open meetings law.[4] Discussion of FOI can properly cover such things as public register laws[5] and information disclosure requirements, such as those in public accounts and companies law.

Complete and unfettered freedom of information is unattainable. It is also, in a free and democratic society, undesirable. There can be "too much of a good thing" in terms of

---

1 I might add that the official information legislation has featured as one strand in the privacy forums I have held annually since 1994. I can only recall one conference on the Official Information Act in that period.

2 Registrations at time of writing have come from Australia, Belgium, Denmark, France, Germany, Hong Kong, Hungary, Ireland, Japan, Malaysia, New Zealand, Portugal, Singapore, Sweden, Thailand and the USA.

3 Roughly speaking, the OIA covers the central government while LGOIMA covers local government. The Privacy Act covers both the public and private sectors.

4 Open meetings laws are sometimes called "sunshine laws". The New Zealand Public Health and Disability Act 2000, is another example of an open meetings law (in respect of District Health Boards).

5 An extensive, although incomplete, list of laws creating public registers is to be found in Privacy Act 1993, Second Schedule.

enforced transparency. Would anyone wish to live in a glass house without curtains? Every FOI law in the world sets limits on what is to be made freely available. Such limits include the coverage of the law itself,[6] the range of rights and duties[7] and the reasons for limiting disclosure where other important public interests need to be protected. A typical access law will recognise many reasons for withholding information such as the needs of law enforcement authorities to protect their informants and to complete investigations without tipping people off. This Symposium focuses upon one of the most important of the limits on FOI rights: the fundamental human right to privacy.

The interface between freedom of information legislation and privacy protection reveals a tension. The issue should not be overstated: the appetite of Open Government can usually be satisfied while reconciling the competing interests. Indeed, I might go so far as to say that the difficult cases reflect a "healthy conflict". After all, one might well suspect that if contests did not occasionally arise, that either the reach of the access law was unduly limited or that arbitrary rules required the surrendering of privacy too readily. (On the other hand, one wishes to avoid unnecessary conflict on routine matters by training of officials, clear administrative guidelines and dissemination of instructive casenotes.)

Origins, background, scope

The Symposium begins with an examination of the origins, background and scope of freedom of information, personal access and data protection law. In "Convergence, Divergence or Parallel Tracks?" Grant Liddell, sets the scene. Grant is well qualified to lead off proceedings given his experience as Crown Counsel and law teacher, as well as roles as adviser to the former Information Authority and co-author of an FOI law text. Grant has taken a lively interest in privacy in his writings and public speaking and been involved in litigation touching upon the Privacy Act and Health Information Privacy Code 1994.

FOI/privacy law interrelationships

Following the introduction, the Symposium examines the practical inter-relationship between the FOI and privacy laws. In this panel, Judge Satyanand joins me in discussing the consultation processes between the Ombudsmen and my office in the resolution of OIA cases raising privacy issues. A practitioner in information law, with credentials in both privacy and official information, John Edwards, completes the New Zealand perspective by reflecting on the purpose of FOI law and the need to effectively protect privacy interests. Panellists from Thailand, Chungtong Opassiriwit, and Australia, Rick Snell, inform the Symposium about other models for handling the inter-relationship between FOI and privacy laws. Thailand operates a combined FOI data protection review authority while Australia accords individuals the powerful right to initiate a "reverse FOI appeal". The pros and cons of each approach will no doubt foster lively

---

6 For example, the OIA applies only to most, not all, public bodies. It does not apply to private bodies. Other laws specify the information types that are covered, for example public register laws list the information to be contained in the register open to search. Some other laws confer rights on certain authorised persons to have access to information but restrict access by others: for example, the Mental Health (Compulsory Assessment and Treatment) Act 1992 and the Victims of Offences Act 1987, each list certain people to be notified of certain proceedings.

7 For example, at a fairly fundamental level, access to information laws entitled requests to be made for information that exists but did not generally oblige officials to go out and find answers and create information in documents to benefit the individual requester.

discussion amongst an audience which includes access review authorities from Europe, , Asia and Australasia.

Proactive dissemination

Following the coffee break, the Symposium tackles an area where New Zealand arguably lags behind others: proactive dissemination of publicly held information. While the OIA covers the classic "request and response" aspects of FOI law, citizens who don't know of the existence of documents are unlikely to request them. Policies of "routine disclosure/active dissemination" require public bodies to anticipate the public interest and to seek to satisfy it. Well designed RD/AD policies are cost effective, timely and can anticipate and resolve privacy issues by pre-empting conflict on an access request. David Smith, from the UK Information Commissioner's office, outlines the new publication scheme requirement in that jurisdiction's new FOI Act. Bronwyn Keighley-Gerardy, Western Australia's Information Commissioner, emphasises active education and assistance to departments and requesters.

Evelyn Wareham canvasses some aspects of FOI and privacy as they relate to the vast repository of public records held in archives. While being of interest in its own right, best archival practice in terms of finding aids and retrieval methods, and the new access standard, may offer lessons for information access during the rest of a document's lifecycle.

Dispute resolution

If privacy is not simply to be a casualty of an unthinking desire for openness – a tyranny of transparency – it is necessary to articulate the important public interest in upholding privacy and apply an approach to protect that interest. It is essential to provide mechanisms to enable disputes to be resolved. As the President of the French Data Protection Commission put it:

> *States must ensure respect for private life for everyone and also transparency of public action, which is essential for the good functioning of a democratic society.*
>
> *The tension that may, however, exist between access to administrative information, or, more generally, information that is made public, and the protection of personal data can be resolved. [E]xamples... taken from experience, show that reconciliation is possible. This, however, requires a solid legal basis, and a case by case examination that is both prospective and technological.*
>
> *This attempt at reconciliation also requires that States agree – as they cannot be both a party and a judge – to leave the task of arbitration between the often conflicting interests of the administration of the citizen, in the hands of independent institutions.*[8]

Associate Professor Paul Roth, of the Faculty of Law at the University of Otago, discusses the access review processes for personal and third party requests in New Zealand law under the OIA and Privacy Act. This involves complaint to my office or the Ombudsmen's. The Privacy Act additionally allows for recourse to a tribunal in certain circumstances.

---

[8] Michel Gentot, President of the Commission Nationale de l'Informatique et des Libertés, "Access to Information and Protection of Personal Data" in Conference Proceedings of 21st International Conference on Privacy and Personal Data Protection, Hong Kong SAR, September 1999.

Chris Puplick, New South Wales Privacy Commissioner, outlines the dispute resolution processes in that State which include, on the privacy side, standards for internal complaints handling. Appeals under both the personal access and third party access laws can be taken to the Administrative Decisions Tribunal. We are fortunate to have Judge Kevin O'Connor giving a perspective on the usefulness of a judicial component in FOI and data protection dispute resolution. Judge O'Connor will be familiar to New Zealand privacy audiences as Australia's first Privacy Commissioner and speaker at several privacy forums. His credentials in the area are substantial: he was the principal researcher on the highly regarded Australian Law Reform Commission *Privacy* report. Kevin O'Connor's elevation to the judiciary after completing his terms as Privacy Commissioner was well deserved and in his role as President of the ADT he can receive appeals under the State's FOI law and under its new privacy law.

Special access regimes

FOI law does not start and stop at the OIA and Privacy Act. Blair Stewart, Assistant Privacy Commissioner, leads discussion of certain special access regimes with a brief look at how New Zealand public register access laws address privacy issues. Dr Ulf Brühann touches upon access rights at the supranational level in the European Union. The EU has reached an advanced point by according rights to access information held by community institutions. Such access rights relate both to individuals and the information held about them and third party FOI rights.

Well known journalist and commentator on media practice and ethics, Jim Tucker, touches upon the always contentious and topical subject of the New Zealand courts' approach to name suppression.

Finally, Dr Alexander Dix discusses the extraordinary circumstances posed by the Federal Republic's inheritance of East Germany's secret police files. Germany, which has built a thorough reputation in its handling of human rights and data protection issues, has taken a determined, sophisticated and sometimes controversial approach to the files. Considerable resource has been put into maintaining and indexing the files to facilitate individual access by the victims of the Stasi.

Perspectives from some OIA users - researchers - journalists

The afternoon sessions commence with a presentation from Nicky Hager, best known in privacy circles for his 1999 book *Secret Power: New Zealand's Role in the International Spy Network*. Controversy resulting from publication led to a year long investigation by the European Parliament. Part of the information for the book was obtained under the OIA. However, it might have been difficult to write a comprehensive and revealing book based solely on such sources. Covert agencies operating in the interests of national security are another of the "flash points" for FOI law. Eugene Bingham, a senior journalist with the *New Zealand Herald*, gives the perspective of a regular user of the OIA to obtain information for daily newspaper purposes.

There are a range of views about journalistic use of the OIA. Journalists for daily newspapers often complain that it doesn't pay heed to their copy deadlines. Feature writers and investigative journalists may have more success so long as they are willing to persevere. Personally, I suspect that too few journalists take the time to study the OIA,

or are trained in it by their employers, to make effective use of the Act. For one thing, there is no need for an OIA request to be in writing – and journalists may not realise that requests may on occasion be successful on the phone. Such matters come to my attention where a journalist has been fobbed off by a bureaucrat and the journalist has been misled into taking the well trodden path of writing a Privacy Act "explanation". Frequently the journalist is in total ignorance of the legal duty under the OIA to give reasons for refusing the request.[9] Reasons given must be precise and in the terms allowed for in the OIA itself. For example, it is not permissible, and legally quite wrong, for an OIA request to be refused with an explanation that "the Privacy Act doesn't allow me to tell you that". An essential skill for a journalist in 2002 is a good working knowledge of the OIA. The journalist should challenge the bureaucrat to specify the reason and give the grounds in support. It is perfectly true that the OIA reason for refusal may be that it is necessary for the information to be withheld to protect the privacy of a natural person and that there is no countervailing public interest requiring disclosure. However, that is a long way from being "fobbed off with the Privacy Act" as newspapers are quick to allege. In such reasons for a refusal the Privacy Act plays no part.

A second area where some journalists seem unaware of the OIA requirements is the time for making decisions. Too frequently I hear journalists saying the OIA is no use because it allows 20 working days to give a decision. However, the legal duty is to give the decision "as soon as reasonably practicable".[10] That can include an immediate over- the-counter or over-the-telephone decision which can then be taken on review to the Ombudsman. Subject to the pressures on staff at the time, it is not out of the question that an Ombudsman's intervention might actually secure access to the information well within the 20 working days (so long as it is a straightforward case that does not require formal investigation). Even if the Ombudsman needs to investigate, it is conceivable that the investigation will be started within that 20 working day period.[11]

Drawing together the strands

From mid-afternoon on, the Symposium draws various strands together starting in a roundtable discussion involving the Privacy Commissioner and Ombudsman, and a panel of experts from around the world. The panel includes Nigel Waters, a privacy expert from Australia and Associate Editor of *Privacy Law & Policy Reporter*, and also a number of others will join the panel from the international expertise assembled for the Symposium.

In the final session, the panel looks to the future. Blair Stewart, Assistant Privacy Commissioner, is joined by another New Zealand panellist, Tim McBride. Mr McBride has been actively involved in the privacy area in New Zealand for many years as an advocate, author, barrister, commentator, consultant and lecturer. They are joined by Paul Chadwick, newly appointed Victorian Privacy Commissioner, with a background as a journalist and lawyer who has written books on FOI and media ownership. Dr Hansjürgen Garstka, Data Protection and Access Commissioner for the Berlin State,

---

9 OIA, s.19.

10 OIA, s.15(1).

11 In making these comments I am merely illustrating some journalists' lack of familiarity with the OIA. I am not suggesting it is always best practice to press officials to give immediate decisions over the telephone. Nor should it be thought that the Ombudsmen will always be able initially to deal with a matter within days of receiving it.

joins to the discussion and focuses on the opportunities for sharing experiences on FOI and privacy issues. This links to the fact that there are an increasing number of privacy and data protection commissioners, throughout Europe and Canada who perform general FOI-type access review functions.

Finally, Brian Pink, the New Zealand Government Statistician, will offer a personal reflection on the day's events.

Acknowledgements

I record my profound thanks for the contribution of all speakers and panellists. I am also grateful to Chapman Tripp for their sponsorship which covered the cost of the sound system and microphones for the day and to LexisNexis Butterworths for supply of pads and pens.

FREEDOM OF INFORMATION AND PRIVACY: COMPETING INTERESTS WITH COMPLEMENTARY AIMS

Bruce Slane
New Zealand Privacy Commissioner

Public sector agencies must attempt to balance the competing interests of the desirability of freedom of official information with the need to provide sufficient protection to personal privacy.

Privacy policies

As far as personal information about identifiable individuals is concerned, public sector agencies' information policies are governed by the information privacy principles set out in the Privacy Act 1993. A good deal of discretion is left with agencies to develop the scope and characteristics of their own policies.

However the policies should be open and transparent and those whose personal information is being held by the agency should be made aware of the purposes for which it has been obtained and for which it may be used or disclosed. This openness introduces accountability and a quite proper democratic pressure to be fair and reasonable in those information handling practices.

Openness and accountability are essential ingredients of the privacy principles. But nothing in the principles derogates from any statute or regulation which authorises or requires information to be collected or disclosed. The Official Information Act 1982[1] is such a statute. Although dealing in different areas, the Privacy Act and the Official Information Act have similarities. The two statutes work in together, for the most part, in harmonious accord.

Information requests: three routes

In broad terms, requests are dealt with according to the type of information the requester seeks.

- Requests made **by individuals for information about themselves** must be dealt with in accordance with principle 6 of the Privacy Act. The Privacy Act also contains the only grounds for withholding that personal information if the agency wishes to do so.

- Where a request is made **by a non-natural person, such as a company, for information about itself,** similar provisions in Part IV of the Official Information Act apply.[2]

---

1 References to the Official Information Act include references to the corresponding sections in the Local Government Official Information and Meetings Act 1987.

2 Historically, requests for personal information by natural persons were also dealt with under the Official Information Act 1982, s 24(2). This access regime did not extend to the private sector. The personal access right for natural persons was removed from the OIA by the Official Information Amendment Act 1993, s 5(2). Expanded personal access rights were provided for in the Privacy Act 1993.

- When a request is made for **official information** (i.e. not personal information about the requester) and the information is not normally routinely given out, the agency must consider the request under the Official Information Act. If the information requested contains personal information about identifiable individuals or may otherwise infringe the privacy of individuals, then the provisions and withholding grounds of the *Official Information Act* will govern a decision to release that information or not.

Principle of availability

The key underlying principle of the Official Information Act is that information shall be made available unless there is good reason for withholding it.[3] Except where the Act otherwise expressly requires, questions of availability of official information should be decided in accordance with the purposes of the Official Information Act. The information should be supplied "as soon as practicable", and in any case no later than 20 working days.

It is important to note, however, that under section 4 of the Official Information Act, one of the Act's purposes is to "protect official information to the extent consistent with the public interest and the preservation of personal privacy".

Good reasons for withholding: privacy

One good reason for withholding official information is to protect the privacy of natural persons, including that of deceased natural persons (section 9(2)(a)). Relying upon this withholding ground involves a three-stage process:

1. identification of the strength of any privacy interest;
2. identification of the strength of any public interest supporting disclosure (or, on occasion, supporting withholding the information);
3. weighing the competing interests.

Necessary to withhold?

In considering whether it is necessary to protect the privacy of a natural person, agencies may well look to principle 11 of the Privacy Act for assistance. For instance, an agency may see an exception in rule 11 which could apply. However using the exception to disclose information may imperil the relationship the organisation has with those who supplied the information, or may be contrary to long-standing, well-understood policies. The agency may decide, for instance, that instituting debt collection proceedings is not sufficient justification to supply name and address information to plaintiffs. It may also be useful to examine the purposes for which the information was obtained and to see whether acceding to the request would be consistent with those purposes. However, principle 11 does not determine the issue.

If the agency decides that it is *necessary* to protect privacy interests, then the agency must consider whether, in the circumstances of a particular case, withholding the information is outweighed by other considerations which render it desirable, in the public interest, to

---

[3] Official Information Act 1982, section 5.

make that information available.[4] This is a balancing exercise which must be sincerely entered into if the disclosure is to obtain protection against any subsequent complaint to the Privacy Commissioner. If information is released under the Official Information Act in good faith, a complaint about the disclosure cannot be upheld under the Privacy Act.

Review of decision

If an agency decides to withhold the information, the requester may take the matter to the Ombudsman for review. Where information is being withheld on the basis of a privacy interest, the Ombudsman must consult the Privacy Commissioner before forming a final opinion.[5]

That consultative process often includes considering:

- the purposes for which the information is held; whether it has been acquired under some coercive statute or voluntarily supplied, whether the individuals concerned have been approached or can be approached for their reaction to the request;
- the public interest reasons put forward by the requester;
- any other public interest reasons (such as accountability) which favour release;
- any public interest factors which favour withholding the information;
- any conditions that can effectively be imposed on the requester to limit any further infringement of privacy.

In the last 4 years there have been between 50 and 77 consultations annually between the Ombudsmen and Privacy Commissioner.

Joint investigations

Sometimes a request is made for both personal information about the requester and for official information. In those cases, investigating officers of the Privacy Commissioner and the Ombudsman work together to separate the two types of information and apply the appropriate provisions of the respective Acts to it. Usually one office will be used as a conduit for the correspondence on both the personal and official information.

The Ombudsman's Practice Guideline No.6 sets out how the Ombudsmen approach requests for official information and deal with the privacy withholding ground.

---

4 Official Information Act 1982, section 9(1).

5 Official Information Act 1982, section 29B; Local Government Official Information and Meetings Act 1987, section 29A.

INTERFACE BETWEEN THE OFFICIAL INFORMATION AND PRIVACY ACTS

Judge Anand Satyanand,
Ombudsman, New Zealand

1. The Official Information Act applies to all information held by public sector agencies that are subject to the Act. This includes departments, ministries, crown entities, state-owned enterprises, ministers of the crown, local authorities, district health boards, school boards of trustees and tertiary institutions.

2. By definition, personal information held by public sector organisations is a subset of official information. The interface between the Official Information Act and the Privacy Act is limited to the extent that the information at issue comprises or includes personal information about a natural person.

3. For public sector agencies subject to the Official Information Act, the interface occurs:
   - on receipt of a request, when they must determine which Act applies; and
   - in making a decision whether to grant the request, when the agency must decide whether there is good reason to refuse the request in order to protect personal privacy.

4. In general terms the Official Information Act provides a code as to when requests for information may be refused. Section 5 of the Official Information Act provides that:

   > *The question whether any official information is to be made available where that question arises under this Act, shall be determined, except where this Act otherwise expressly requires, in accordance with the purposes of the Act and the principle that the information shall be made available unless there is good reason for withholding it.*

5. Whether there is good reason to withhold information in order to protect the privacy of natural persons is governed by section 9(2)(a) of the Official Information Act. Section 9(2)(a) will provide good reason to withhold information if, and only if:
   - The withholding of the information is necessary to *"protect the privacy of natural persons, including that of deceased natural persons"*; and
   - This interest is not *"outweighed by other considerations which render it desirable, in the public interest, to make that information available"*.

   When considering whether it is necessary to withhold specific information each case must be considered on its own merits. While an agency's general or historical practices may be relevant in this regard, they are not determinative. The fact that a practice is long standing does not necessarily mean that it is justified in the circumstances of every case.

6. Section 9(2)(a) reflects one of the purposes set out in section 4 of the Act, which is to *"protect official information to the extent consistent with the public interest and the*

preservation of personal privacy". However, section 9(2)(a) is subject to section 9(1). This means that even if there is a privacy interest in the information that requires protection, the agency must still consider whether, in the circumstances of the case, the public interest requires disclosure of the information in any event.

7. The test to be applied under section 9(1) is whether the considerations favouring disclosure outweigh, in the public interest, the need to withhold the information to protect privacy. The exercise is not so much one of balancing competing interests, but rather assessing the weight of competing interests in the circumstances of a particular case.

8. In making that assessment, matters such as:
   - accountability for a decision being made;
   - transparency of a process; and
   - ensuring that natural justice is accorded;

   may be relevant to a consideration of whether the public interest requires release of information.

9. Privacy issues often arise in the context of situations where information is requested in order to:
   - challenge allegations of impropriety or illegality;
   - challenge decisions or recommendations made in an employment context;
   - enable parents to access meaningful information from their children's school records; and
   - obtain information about remuneration in the public sector.

   In some cases there may be a public interest in releasing sufficient information to enable requesters to fulfil these objectives, notwithstanding concerns about personal privacy.

10. While the application of the Official Information Act is triggered by requests for access, the assessment of whether any of the reasons for refusal under section 9(2) apply usually turns on the purpose for which the information may be used. Similarly, the purpose for which the information may be used will also be relevant when identifying and weighing competing considerations under section 9(1).

11. The right under section 23 of the Official Information Act to obtain a statement of reasons for decisions and recommendations provides a very clear illustration of the importance of knowing how information has been used.

12. In respect of the Ombudsman's role in reviewing decisions to withhold information pursuant to section 9(2)(a), there is a statutory requirement to consult the Privacy Commissioner before forming a final view that the request should not have been refused. In this regard, there has been nearly a decade of experience of such consultation between the Ombudsmen and the Privacy Commissioner.

13. The Ombudsmen's general approach to the application of section 9(2)(a) of the Official Information Act is covered in the Practice Guidelines that the Office of the Ombudsmen publishes from time to time.

THAILAND: A CASE STUDY IN THE INTERRELATIONSHIP BETWEEN FREEDOM OF INFORMATION (FOI) AND PRIVACY

Chungtong Opassiriwit
Director
The Office of the Official Information Commission (Board)
and Secretary to
the Information Disclosure Tribunal
Thailand

Contents

1. Constitution of the Kingdom of Thailand, B.E. 2540 (1997)

Thailand Constitution (1997) has define principle to protect people right to know and Privacy as mention in the constitution

1.1 A persons family rights, dignity, reputation or the right of privacy shall be protected.
The assertion or circulation of a statement or picture in any manner whatsoever to the public, which violates or affects a person's family rights, dignity, reputation or the right of privacy, shall not be made except for the case which in beneficial to the public. (section 34)

1.2 A person shall have the right to get access to public information in possession of a State agency, State enterprise or local government organization, unless the disclosure of such information shall affect the security of the State, public safety or interests of other persons which shall be protected as provided by law. (Section 58)

1.3 A person shall have the right to receive information, explanation and reason from a State agency, State enterprise or local government organization before permission is given for the operation of any project or activity which may affect the quality of the environment, health and sanitary conditions, the quality of life or any other material interest concerning him or her (section 59)

2. *Official information Act (OIA), B.E. 2540 (1997)*

The official information Act (1997) of Thailand has four important objectives.

2.1 To ensure people's right to know state agency information in order to :
(1) People can view their opinion and use their political right correctly
(2) Promoting transparent and efficient government.
(3) Promoting Democratic stability.

2.2 To define clearly what kind of official information may not Subject to Disclosure

2.3 To protect the Personal information which possess or control by a state agency.

2.4 To secure Historical information

3. The boundary of Official Information and State agency

3.1 Official information
Means an information in possession or control of a State agency, whether it is the information relating to the operation of the state or the information relating to a private individual;

3.2 State agency
Means a central administration, provincial administration, local administration, State enterprise, Government agency attached to the National Assembly, court only in respect of the affairs unassociated with the trial and adjudication of cases. Professional supervisory organization, independent agency of the State and such other agency as prescribed in the Ministerial regulation;

4. The Official Information Act and the principle of People Right to know

The Act has set three principles for information disclosure.

4.1 A State agency shall at least publish the following official information in the Government Gazette: (OIA, section 7 Paragraph one)
(1) the structure and organization of its operation: (OIA, section 7)
(2) the summary of important powers and duties and operational methods; (OIA, section 7(2))
(3) a contacting address for the purpose of contacting the State agency in order to request and obtain information or advice; (OIA, section 7(3))
(4) by-laws, resolutions of the Council of Ministers, regulations, orders, circulars, Rules, work pattern, policies or interpretations only insofar as they are made or issued to have the same force as by-laws and intended to be to general application to private Individuals concerned; (OIA, section 7 (4))
(5) such other information as determined by the Board. (OIA, section 7 (5))

A State agency shall, for dissemination purpose, compile and make available the information under paragraph one for sale, disposal or distribution at its office as it thinks fit.

4.2 Make available at least the following official information for public inspection: (OIA, section9 Paragraph one)
(1) a result of consideration or a decision which has a direct effect on a private individual including a dissenting opinion and an order relating thereto: (OIA, section 9(1))
(2) a policy or an interpretation which does not fall within the scope of the requirement of publication in the Government Gazette under section 7 (4): (OIA, section 9 (2))
(3) a work-plan, project and annual expenditure estimate of the year of its preparation; (OIA, section 9(3))
(4) a manual or order relating to work procedure of State officials which affects the rights and duties of private individuals; (OIA, section 9(4))
(5) a concession contract, agreement of a monopolistic nature of joint venture agreement with a private individual for the provision of public services; (OIA, section 9(6))
(6) a resolution of the Council of Ministers or of such Board, Tribunal Commission or Committee as established by law or by a resolution of the Council of Ministers; provided that the titles of the technical reports, fact reports or information relied on in such consideration shall also be specified; (OIA, section 9 (7))
(7) such other information as determined by the Board. (OIA, section 9 (8))
A person, whether interested in the matter concerned or not , has the right to inspect or obtain a copy or a certified copy of the information under paragraph one.

4.3 Provide information to individual request:
If any person making a request for any official information other than the official information already published in the Government Gazette or already made available for public inspection or already made available for public studies and such request makes a reasonably apprehensible mention of the intended information, the responsible State agency shall provide it to such person within a reasonable period of time, unless the request in make for an excessive amount or frequently with out reasonable cause.(OIA, section 11))

5. The information that may not be disclosed

We can see that most of the official information is subject to disclose while only few is declared as an exemption. According to the Official Information Act, some information, which is not subject to disclosure, is described as follows

5.1 Official information which may jeopardize the Royal Institution shall not be disclosed. (OIA, section 14)

5.2 A state agency or State official may issue an order prohibiting the disclosure of official information falling under any of the following descriptions. Having regard to the performance of duties of the State agency under the law, public interests and the interests of the private individuals concerned: (OIA, section 15)
(1) the disclosure thereof will jeopardize the national security, international relations, or national economic or financial security; (OIA, section 15 (1))
(2) the disclosure there of will result in the decline in the efficiency of law enforcement or failure to achieve its objectives, whether or not it is related to

litigation, protection, suppression, verification, inspection, or knowledge of the sure of the information; (OIA, section 15 (2))
(3) an opinion or advice given within the State agency with regard to the performance of any act, not including a technical report, fact report or information relied on for giving opinion or recommendation internally; (OIA, section 15 (3))
(4) the disclosure there of will endanger the life or safety of any person; (OIA, section 15 (4))
(5) a medical report or personal information the disclosure of which will unreasonably encroach upon the right of privacy; (OIA, section 15 (5))
(6) an official information protected by law against disclosure or an information given by a person and intended to be kept undisclosed; (OIA, section 15 (6))
(7) other cases as prescribed in the Royal Decree. (OIA, section 15 (7))

An order prohibiting the disclosure of official information may be issued subject to any condition whatsoever, but there shall also be stated therein the type of information and the reasons for non-disclosure. It shall be deemed that the issuance of an order disclosing official information is the exclusive discretion of State officials in consecutive levels of command; provided that, a person who makes a request for the information may appeal to the Information Disclosure Tribunal as provided in the Act. (OIA, section 15 Paragraph two)

6. The protection of the Personal Information and the Official Information Act

The Act state that all the state agency:

6.1 A State agency shall take the following actions with regard to the provision of a personal information system:

(1) providing for a personal information system only insofar as it is relevant to and necessary for the achievement of the objectives of the operation of the State agency, and terminating the provision thereof whenever it becomes unnecessary;

(2) making efforts to collect information directly from the person who is the subject thereof, especially in the case where such person's interests will be directly affected;

(3) causing the following information to be published in the Government Gazette and examining and correcting the same regularly:
   (a) the type of persons in respect of which information has been held;
   (b) the type to the personal information system;
   (c) the ordinary nature of the use of the information;
   (d) the procedure for the inspection of the information of the person who is the subject thereof;
   (e) the procedure for the making of a request for the correction and alteration of the information;
   (f) the source of the information;

(4) examining and correcting personal information under its responsibility;

(5) providing an appropriate security system for the personal information system in order to prevent improper use of any use to the prejudice of the person who is the subject of the information.

In the case where the information has directly been collected from the person who is the subject thereof, a State agency shall, in advance or simultaneously with the request therefore, notify such person of the purpose for the use of the information, the ordinary nature of its use and whether such case of making the request is one which the information may be given voluntarily or one which it must be given compulsorily under the law. (OIA, section 23 paragraph two)

In the case where the personal information is dispatched to any place which, in consequence thereof, may become known to general members of the public, a State agency must notify the person who is the subject thereof, unless it is carried out in conformity with the ordinary nature of the use of the information (OIA, section 23 paragraph three)

6.2 A State agency shall not disclose personal information in its control to other State agencies or other persons without prior or immediate consent given in writing by the person who is the subject thereof except for the disclosure in the following circumstances; (OIA, section 24 paragraph one)

(1) the disclosure to State officials in its own agency for the purpose of using it in accordance with the powers and duties of such agency;
(2) the disclosure in its ordinary use within the objectives of the provision for such personal information system;
(3) the disclosure to State agencies which operate in the field of planning statistics or censuses and have the duty to keep the personal information undisclosed;
(4) the disclosure for studies and research without mentioning the name or part revealing the identity of the person to whom the personal information is related.
(5) the disclosure to the National Archives Division, Fine Arts Department or other State agencies under section 26 paragraph one for the purpose of evaluating the value of keeping such information;
(6) the disclosure to State officials for the purpose of preventing the violation of law or non-compliance with the law, conducting investigations and inquiries or instituting legal actions of any type whatsoever;
(7) the disclosure necessary for the prevention or elimination of hazards to the life or health of persons;
(8) the disclosure to the Court, State officials, State agencies or persons having the power under the law to make a request for such information;
(9) other cases as prescribed in the Royal Decree;

In disclosing the personal information under paragraph one (3), (4), (5), (6), (7), (8) and (9) a list recording the disclosure shall be prepared and attached to such information in accordance with the rules and procedure prescribed in the Ministerial Regulation.

6.3 A person shall have the right to get access to personal information relating to him. When such person makes a request in writing, the State agency in control of such information shall allow him or his authorized representative to inspect or obtain a copy of the same.

In the case where there exists a reasonable ground to disclose a medical report relating to any person, state officials may disclose it only to doctors entrusted by such person.

A person who considers that any part of personal information relating to him is incorrect shall have the right to make a request in writing to the State agency in control of such information to correct, alter or delete that part of information. The State agency shall consider the request and notify its result to such person without delay.

In the case where the State agency fails to correct, alter or delete the information pursuant to the request, such person shall have the right to appeal to the Information Disclosure Tribunal within thirty days as from the date of the receipt of the notification of the order refusing to correct, alter or delete the same. The appeal shall be submitted through the Board and, in any case, the person who is the subject of the information shall have the right to require the State official to attach his request to the relevant part of the information.

7. The complaint and appeal cases and the Official Information Act

7.1 Complaint case

Any person, who considers that a State agency fails to publish the information under section 7, fails to make the information available for public inspection under section 9, fails to provide him with the information under section 11, violates or fails to comply with this Act, ordeals in performing its duties, or considers that he does not receive convenience without reasonable cause, is entitled to lodge a complaint with the Board, (OIA, section 13)

In the case where a State agency denies that there is such information as requested, if the person so requesting does not believe that it is true and lodges a complaint with the Board (Commission) the Board shall have the power to inspect the relevant official information and notify the complainant of the result of the inspection.

The State agency or State official shall allow the Board or the person entrusted by the Board to inspect the information which is in its or his possession, whether or not it is the information permitted to be disclosed. (OIA, section 33)

7.2 Appeal case

There shall be information Disclosure Tribunals in appropriate fields, which are appointed by the Council of Ministers upon the recommendation of the Board, having the power and duty to consider and decide an appeal against an order prohibiting the disclosure of information. (OIA, section 35)

The appointment of Information Disclosure Tribunals under paragraph one shall be made on the basis of the specialized fields of the official information, such as the fields of national security, national economy and finance or law enforcement. (OIA, section 35)

The decision of an Information Disclosure Tribunal shall be deemed final. In making the decision, an observation may be made to the Board with regard to appropriate action to be taken by the State agency concerned in any particular case. (OIA, section 37)

8. The appeal cases and the decision of an Information Disclosure Tribunal.

8.1 Case : The entrance examination result disclosure (Decision No. S1/1998)

Background

The Parents of a student, who failed the entrance examination for the Demonstration School of Kasetsart University, petitioned the school to disclose the examination result of her daughter and other students. After the school denied releasing, the parents then submitted the appeal to the Office of the Official Information Commission (OIC) to force the school to disclose the requested information.

The case is also concerned with the issue of personal information intervention. As the school claimed that the score and answer sheets were categorized as personal information and couldn't be revealed to anyone else apart from the owner. The parents of other students filed a lawsuit

The Decision

The Information Disclosure Tribunals for Social Information (IDT) ruled that the parents has the rights to see the examination result, but the school, however, declined to comply with the IDT's decision. The school claimed they had to consult the council of State , the Attorney General's Office, and the Ministry of University Affairs first, in order to have guided procedures for disclosing examination result, which should be set up as a new standard to cope with similar request in the future.

Finally, the OIC confirmed the IDT's order and enforced the disclosure, followed by the cabinet's resolution asserting that state agency had to comply with the OIC's recommendations and the IDT's order; otherwise they should be punished by disciplinary regulation.

8.2 Case : Corruption Investigation Report (Decision No. S 15/1999)

Background

Journalists and non-government organization (NGOs) petitioned the office of the Counter Corruption Commission (CCC) to disclose the investigative result report of the corruption in the Ministry of Public Health. The CCC denied disclosing the requested documents; petitioners then submitted the appeal to the office of the official Information Commission (OIC.)

The disclosure of investigative report of the CCC, concerning the corruption scandal in purchasing drug and health materials in the Ministry of Public Health, was criticized as the might hamper the efficiency of law enforcement. It was

argued that the report was protected by the CCC's regulations against disclosure and that concerned witness who gave investigative documents intended their names and those information to be kept undisclosed.

The Decision

The Information Disclosure Tribunals for Social Information (IDT) ruled that the investigation was finalized. Those involved officials were disciplinarily punished and politicians were forwarded to criminal investigation. The IDT considered that the investigative report is official information, and the case has great impact on pubic interest and the disclosure could bring about positive attitude to the national administration, in particular to the CCC itself. The IDT thus decided that the CCC disclosed the requested information.

As a matter of fact, the witnesses in this case were high position executives; their activities as witnesses in this case were official duty of which will be protected by law. Though there is a regulation of the CCC against the disclosure of such information of the argument of witness safety, the discretion of the IDT in this case was weighted over by public interest. As the scandal involved a large amount of national budget, committed by the height-ranking officials, involving high executive members, both government officials and politicians, The case was very sensitive, as it is the corruption of purchasing drugs, which affect basic services to the people, in particular, the poor.

8.3 Case : The Business Contract (Decision No.E2/1998)

Background

Journalists requested to the Financial Sector Restructuring Authority (FRA) to release the Purchasing Contract related to the Bid for sales of the Financial Sector Debits. The FRA refused to release such requested information claiming that the documents were business contracts between the FRA and private company and such a commercial deal cannot be disclosed.

The Decision

After considering this appeal case, the Information Disclosure Tribunal (IDT) for Economic Information ruled the FRA to release the contract with exceptional conditions for Initial Purchase Price and Sharing Agreement to be released after the bid date. Those documents contain personal information, such as amount and information, which are personal debts, should be privacy protected.

8.4 Case : Application documents for constructing a river pier (Decision No. S 17/2000)

Background

A man suspected that the construction of a river pier will not follow river regulation and might be obstruction and damage to river navigation. So he request to get the Application documents for contraction the river pier of a

businessman from the Port Authority. But the port Authority refused to disclose the documents because the documents concern with Personal Data and the disclosure will have bad effected to the business of the Applicant

The Decision

The Information Disclosure Tribunal (IDT) for Social Information ruled that the documents are not the Personal Data but it concern the government permission procedure. And the disclosure will benefit to public and promote confident to the Authority concern.

9. The Implication of Freedom to Information Access vs. Privacy Protection

The Official Information Act is a new law, knowledge and understanding in the Freedom of Information, and Privacy Protection issue, in particular, is new for Thailand. During the first two years of the Information act implementation, there was some implication of misunderstanding of the law substance, and many cases reflected the tension between the matter of freedom of access to information and privacy protection, since these two issues are closely related. On the academic perception, many scholars propose the two issuers to be separately considered while some claim that close interrelationship as two sides of the coin. To the Thailand experience from 1992 -2001, according to the Act, in the matter of information disclosure, discretion of state officials must be made with regards to the factors of State duties, public interests, and private interest. This is also confirmed by the constitution, which stipulated information causing damage to a person, dignity, reputation or privacy must be prohibited. Therefore, freedom of information and privacy protection could be persistently found on each other's boundary and become the matter of how to balance these two components.

PROACTIVE DISSEMINATION OF PUBLICLY-HELD INFORMATION
A BRIEF OVERVIEW FROM WESTERN AUSTRALIA

Bronwyn Keighley-Gerardy
Information Commissioner (WA)

Both the democratic and trust principles demand that government be conducted openly. They require that the public be informed of the actions and purposes of government, not because government considers it expedient for the public to know, but because the public has a right to know...openness in government is the indispensable pre-requisite to accountability to the public.[1]

Introduction

Government information is normally accessible to the public in a number of ways including, the Parliamentary Committee system,[2] through local Members of Parliament, in the Annual Reports of agencies, and Government publications. However, no society can consider itself truly democratic if its citizens must be satisfied only with the information fed to them by their leaders. Freedom of Information exists to give citizens a legal right of access to government records, subject to certain exemptions.

FOI legislation is built around three principles. The first is concerned with human rights and privacy. It enables people to gain access to personal information and to correct that information if necessary. The second is the principle of accountability. It seeks to improve the quality of decision-making in the public sector and to ensure proper scrutiny of the activities of government. The third principle is that of democratic participation. This principle seeks to ensure that timely access is available to information, which is gathered at the public expense and for the benefit of government agencies, so that the public can participate in the policy process and in government itself.

The WA experience

In Western Australia, Freedom of Information legislation emerged from a public crisis in confidence concerning actions of government and certain government agencies in the 1980's. The legislation was enacted in 1993 and is based on the earlier FOI Acts in the Commonwealth and in Victoria. However, Western Australia followed the approach taken in Queensland and appointed an Information Commissioner as an independent statutory officer responsible for the operation of the legislation.

In Western Australia, the Information Commissioner has two distinct statutory responsibilities. These are (i) dealing with complaints about decisions made by agencies in respect of FOI applications and (ii) educating and informing the public and agencies in Western Australia about their respective rights and obligations under the legislation. When I am dealing with complaints

---

1 Report of the Royal Commission into Commercial Activities of Government and Other Matters, Govt Printer Perth, 1992, Part II, para 2.1.3.

2 See Report No 2, Part 2, Commission on Government, December 1995, pp 164-177 on the workings of such Committees in Western Australia, and Recommendation 8.4.3.5 to make the functioning of such Committees more effective.

about access, my role is to act as a 'merits review' tribunal. I conduct my own investigations and make decisions that are binding on the parties concerned.

My office is not large. It consists of 10 members – 5 officers are investigators who deal with complaints, the remainder include an Executive Director, to whom I have delegated administrative responsibilities, and technical and support staff whose functions include providing advice and assistance to agencies and applicants. The services we provide, free of charge include:

- conducting training courses;
- developing targeted workshops and seminars;
- providing assistance, briefings and advice to agencies on FOI;
- visiting country regions, agencies or applicants to resolve particular FOI issues that are creating difficulties;
- answering inquiries and requests from the media; and
- briefing community groups.

My office actively encourages policy development within agencies with a focus on the identification of records which can be disclosed without an FOI request being made so that the obligations on agencies under the FOI Act are minimised and do not adversely affect the day-to-day operations of those agencies. Training courses and advisory services are delivered by staff in my office with wide public sector experience and knowledge of the practical problems faced by FOI administrators. However, investigators are not involved in the delivery of advisory services and vice versa. This ensures the impartiality and integrity of the complaint process.

We strive to maintain our credibility at all times with stakeholders and conduct our activities according to the following principles or values:

- being accepted by stakeholders as an independent and impartial review authority;
- being recognised by agencies as a model of best practice for the FOI complaint process;
- serving as an example to agencies of accountability and responsibility;
- providing optimal advisory services to the community as determined by our legislative mandate;
- providing programs and services in the most cost-effective manner.

Making more government information publicly available

Government agencies are the custodians of a vast amount of information upon which decisions are based which can profoundly affect, for better or worse, the lives of ordinary citizens. From time to time, citizens want to know what information about them is on record; they want to know why planning decisions have been made that affect the quality of their lives; why schools and police stations have been closed; why hospitals do not appear to be functioning effectively; why they are expected to obey new rules; why new laws are necessary to regulate their lives; why industry is encroaching on the environment; who makes decisions in government agencies and on what basis; what information is important in the processes of deciding policies and why it is important.

FOI should not be the only way of obtaining access to this kind of information. It may be the preferred option when a decision about whether or not to disclose a document involves complex issues or a more structured approach to decision-making is necessary. Agencies often complain that FOI is too complex, too time-consuming, that it is not a part of their core

business, and that it involves too much work for too little result. However, a simple change in administrative policy, which involves the proactive disclosure of documents, can alleviate the administrative burden of complying with FOI requests and it can strengthen the principle of democratic participation in government.

In theory, the accountability infrastructure in government, of which FOI is a part, should operate in advance to improve public administration. In other words, the mere existence of Ombudsmen, Information Commissioners and the like, should influence government agencies to change their practices. Whilst there are signs that this is happening in some agencies, the problem lies in the accurate measurement of change and in the identification of the degree to which change can be attributed to FOI.[3] Anecdotal evidence suggests that the proactive disclosure of information would not have occurred in WA to the extent that it has without FOI.

My staff and I have worked tirelessly over the past 8 years to cultivate a new culture of openness in the WA public sector. During that time, I have seen a gradual change in the culture of the public sector in WA, from one of endemic secrecy to one where more and more information is becoming routinely available outside the FOI process. There are also encouraging signs that accountability and openness are permeating decision-making at the highest levels. For example, under the previous Liberal Government, the FOI Act was extended to include documents belonging to private contractors responsible for the management of a private prison; the transportation of prisoners; and court security in WA.

A new Local Government Act specifies a range of documents, which local authorities are required to make available to the public. To my knowledge in Australia, the WA Department of Justice was the first government agency to post on its website, a contract for the construction of the State's first private prison. More recently, the new Labor Government, made publicly available on the government web site a contract for the construction of a convention centre in Perth. These WA initiatives have been followed by agencies in other States.

Obstacles and solutions

It is preferable for government agencies to take initiatives, such as those outlined, and make information and documents routinely available, rather than to be forced into disclosing documents by a decision of the Information Commissioner or a court or a tribunal. However, the message my office receives through regular surveys is that the greatest obstacle preventing agencies from making more documents and information freely available is the perceived lack of adequate protection from any litigation, which may arise from such disclosure. I also consider that the continued existence of secrecy provisions in legislation undermines the goals of FOI. It is imperative that the first of these issues is addressed by strengthening the existing provisions in the FOI Act, which give some reassurance to agencies providing disclosures are made in good faith and under the FOI process. The second obstacle needs to be addressed by repealing outdated secrecy provisions in other legislation.

Regardless of the benefits of a more open and accountable system of public administration, it is apparent in some jurisdictions that government agencies prefer to adopt the line of maximum resistance in the faint hope that FOI might disappear from the administrative landscape or be otherwise effectively neutered by government. There is no doubt that without an independent external FOI monitor, there is always a danger of FOI being marginalized and ignored.

---

[3] See the study by Margaret Allars, Associate Professor of Law, Faculty of Law, the University of Sydney reported at the Info One Conference in Adelaide, 22-24 September 1993.

However, there is much that agencies can do to increase the positive benefits from being open and accountable, whilst reducing the administrative burden of FOI. Examples include routinely releasing information without the need for an FOI application; developing an effective and efficient records management system; developing new policies to identify records suitable for routine release; and using the FOI process as an option of last resort rather than the preferred means of addressing the needs of citizens for information.

Further, as new legislation is developed by the public sector or significant amendments are proposed to existing legislation, the opportunity exists to identify those records and documents, which should be publicly available, and to include specific provisions within the legislation itself relating to the public availability of those records.

To achieve a cultural change and a shift in the mindset of government agencies, the three principles of FOI need to be reflected in management values, incorporated into practices, and included as outcomes in public administration.

The French philosopher Paul Valery said: "The future is not what it used to be". Today we have at our disposal new tools, including the internet, to facilitate the dissemination of government information. The only drawback is a failure to acknowledge that information acquired or generated by public officials is not acquired or generated for their own benefit, but for the service of the public.

FREEDOM OF INFORMATION: THE ROLE OF PUBLICATION SCHEMES IN THE UK

David Smith
Assistant Commissioner
Information Commissioner's Office, United Kingdom

Publication schemes are a novel feature of the UK Freedom of Information Act. The nearest parallel is the requirement for a reference book which is contained in the Republic of Ireland's FOI legislation. All UK public bodies, from the largest of central government departments to individual medical practitioners such as dispensing opticians, will have to operate a publication scheme which defines information which they will make available proactively.

The requirements for publication schemes are found in the FOI Act sections 19 and 20. It is the first duty placed on public authorities to come into force, and the production of schemes will be phased - Central Government being first in November 2002.

The full timetable is as follows:

November 2002:	Central Government (except the Crown Prosecution Service and Serious Fraud Office), Parliament, National Assembly for Wales, Non-departmental Public Bodies currently subject to the Code of Practice on Access to Information.
February 2003:	Local Government (except police authorities)
June 2003:	Police, Police Authorities, Crown Prosecution Service, Serious Fraud Office, Armed Forces
October 2003:	National Health Service
February 2004:	Schools, Universities, remaining Non-departmental Public Bodies
June 2004:	Remaining public authorities

The individual right to request information will be available from January 1st 2005.

Basic facts about a publication scheme:

- It is a document approved by the Information Commissioner.
- It has to be published by the public authority. In practice, it will probably be delivered over the internet.
- It details classes of information, categories which group together data which share a common and identifiable attribute or attributes.
- It explains how this information will be published, in what format, and whether a fee will be charged for access to information.

- It will be subject to reapproval every three years, with the expectation that schemes will be reviewed and expanded, especially when individual rights become available.

While all public authorities are entitled to develop their own scheme, and no two schemes are likely to be identical, work has already begun on model frameworks for local government. It is expected that later phases of publication scheme implementation will involve the development and adoption of model schemes in consultation with the Commissioner's Office.

Important features:

- It means that a broad picture of what information is available will be gathered together in one place.

- It provides an opportunity for organisations to reassess what information they make available.

- It provides an opportunity for organisations to publish information for the first time, and to start to consider on an ongoing basis what new information they should publish in the public interest.

- It gives public authorities the opportunity to publish information about their organisation to clarify and improve the public's perception of them.

- It helps create a climate where openness and transparency become increasingly part of a public authority's routine, by requiring them to consider the practical reasons why information should be withheld (and realising in many cases that it can be disclosed)

Benefits to organisations:

- Identifying and publishing information assists in better information management, a key requirement for all UK public authorities, especially those subject to Electronic Records Management targets.

- Publishing accurate and timely information about an authority's functions and activities can improve the public's perception, by making clear what the authority does, and what it does not do.

- Especially in large organisations, a publication scheme provides an internal communications tool which can be accessed across the organisation as well as more widely

NEW ZEALAND TWINS: ACCESS REVIEW PROCESSES FOR PERSONAL AND THIRD PARTY REQUESTS

Paul Roth
Associate Professor
Faculty of Law, University of Otago

Access rights to personal information developed in a piecemeal fashion in New Zealand. The processes for reviewing decisions on access requests reflects this history. The present institutional arrangements for access review are the product of legislative accretion rather than original design. The result is probably not a model to be emulated elsewhere, as it is not as rationalised as it might be. Nevertheless, the variety of review processes that are in place in New Zealand provides a useful indication of the pros and cons of one mode over another.

Review processes under the Official Information Act 1982[1] and Local Government Official Information and Meetings Act 1987[2]

These processes apply to denied access and/or correction requests in respect to information held by public sector agencies.

- Ombudsman investigates and reviews decision.[3]
- Ombudsman reports and may make recommendation.[4]
- Where Ombudsman makes a recommendation, the agency has a public duty to comply with it 21 working days later unless it is overridden by the executive branch of government (Governor General by Order in Council).[5]
- Requester has right to judicial review in the High Court of such Orders in Council.[6]
- Requester has right to judicial review of original decision after Ombudsman has investigated (ie, where Ombudsman has made no recommendation).[7]
- Appeal right in either case to the Court of Appeal.[8]

Requests for personal information by persons to whom the information relates (where "persons" are limited to bodies corporate) are treated differently. Requests for "personal information",[9] and for the reasons for decisions about persons (natural as well as corporate persons),[10] are subject to legal rights enforceable in a Court of law.

Thus, in the case of access to personal information (by bodies corporate only), there are directly enforceable legal rights of access and correction. Alternatively, and this is the usual course, recourse can be had to the Ombudsman's review process as follows:

---

1 Hereafter "OIA".
2 Hereafter "LGOIMA".
3 Section 28 OIA; s 27 LGOIMA. The investigation procedure is governed by Ombudsmen Act 1975: s 29 OIA; s 28 LGOIMA.
4 Section 30 OIA; s 30 LGOIMA.
5 Section 32 OIA; s 32 LGOIMA.
6 Section 32B OIA; s 34 LGOIMA.
7 Section 34 OIA; s 37 LGOIMA.
8 Section 32C OIA; s 35 LGOIMA.
9 Section 24 OIA; s 23 LGOIMA. Prior to the enactment of the Privacy Act, these provisions also covered natural persons. The Privacy Act, however, took jurisdiction over access and correction rights in respect of personal information about natural persons.
10 Section 23 OIA/s 22 LGOIMA.

- Ombudsman investigates, reports, and may make recommendation.[11]
- If recommendation not complied with, in OIA cases the Ombudsman may report to Prime Minister and House of Representatives;[12] in LGOIMA cases, the Ombudsman informs the complainant of non-compliance with recommendation,[13] and may require a summary of the report to be publicly notified and made available.[14]
- Where there is non-compliance with the Ombudsman's recommendation, the complainant must enforce his or her rights in a Court of law.

Review process under the Privacy Act 1993

Where a "person" is a natural person, access and correction rights in respect of "personal information" fall under the Privacy Act rather than the OIA or LGOIMA. The Privacy Act covers personal information held by both public and private sector agencies.

The review process is as follows:

- Privacy Commissioner attempts to settle complaint where possible.[15]
- Privacy Commissioner investigates and reports to parties, and tries to settle complaint where complaint has substance.[16]
- If settlement not reached, Privacy Commissioner may refer matter to Director of Human Rights Proceedings.[17]
- Director of Human Rights Proceedings decides whether or not to institute proceedings on behalf of the complainant before the Human Rights Review Tribunal.[18]
- Complainant may bring proceedings personally before Human Rights Review Tribunal if Privacy Commissioner or Director of Human Rights Proceedings has found the complaint to be without substance or should not be proceeded with, or the Director of Human Rights Proceedings declines to take proceedings.[19]
- Where complaint concerns an unreasonable charge for access to personal information (private sector only), Privacy Commissioner makes final and binding determinations.[20]
- Tribunal determines matter and may award any of the following remedies:[21]

  (a) A declaration that the action of the defendant is an interference with the privacy of an individual;
  (b) An order restraining the defendant from continuing or repeating the interference, or from engaging in, or causing or permitting others to engage in, conduct of the same kind as that constituting the interference, or conduct of any similar kind specified in the order;

---

11 Section 35(1) - (2) OIA; s 38(1) - (3) LGOIMA.
12 Section 35(4) OIA.
13 Section 38(5) LGOIMA.
14 Section 39 LGOIMA.
15 Section 74.
16 Section 77(1).
17 Section 77(2). Prior to 1 January 2002, the Director of Human Rights Proceedings was known as the "Proceedings Commissioner".
18 Section 82. This Tribunal was known as the Complaints Review Tribunal prior to 1 January 2002.
19 Section 83.
20 Section 78.
21 Section 85(1).

(c) Damages for :
  (i) Pecuniary loss suffered as a result of, and expenses reasonably incurred by the aggrieved individual for the purpose of, the transaction or activity out of which the interference arose.
  (ii) Loss of any benefit, whether or not of a monetary kind, which the aggrieved individual might reasonably have been expected to obtain but for the interference.
  (iii) Humiliation, loss of dignity, and injury to the feelings of the aggrieved individual.[22]

(d) An order that the defendant perform any acts specified in the order with a view to remedying the interference, or redressing any loss or damage suffered by the aggrieved individual as a result of the interference, or both;

(e) Such other relief as the Tribunal thinks fit.

- Appeal right from Tribunal to High Court,[23] with appeal right on issues of law to the Court of Appeal.[24]

Alternatively, where the information concerned is held by a public sector agency, there is a legal right to access and correction directly enforceable in a Court of law.[25] This right was carried over from the OIA and LGOIMA.

Overlapping jurisdictions

Double-handling in the course of review processes occurs in relation to information held by public sector agencies, where the legislation makes provision for consultation between the Ombudsmen and the Privacy Commissioner. The Privacy Commissioner is consulted on the Ombudsman's application of s 9(2)(a) OIA and s 7(2)(a) LGOIMA,[26] which deal with the withholding of official information to "protect the privacy of natural persons, including that of deceased natural persons". Over the past few years, there have been between 50 and 80 such consultations per year.

"Mixed information"

"Mixed information" is information about the requester as well as another individual. This is quite common, as much personal information tends to be about individuals in relation to other individuals. Even when the information is ostensibly limited to information about one individual, if may really be another's opinion or belief about the individual concerned.

The concept of "personal information" is a key one for determining the appropriate jurisdiction, since individuals must use the Privacy Act to obtain information about themselves, whereas third parties must use the OIA and LGOIMA to obtain information about others if the information is held by a public sector agency. "Personal information"

---

22 Section 88(1).

23 Section 123 Human Rights Act 1993 applies by virtue of s 89 Privacy Act.

24 Section 124 Human Rights Act 1993 applies by virtue of s 89 Privacy Act.

25 Section 11(1).

26 See s29B OIA and s 29A LGOIMA. In addition, where the Privacy Commissioner receives a complaint that more properly relates to an area under the Ombudsmen's jurisdiction (see the discussion of "mixed information" below), s 72 of the Privacy Act requires the Privacy Commissioner to consult the Chief Ombudsman with a view to possible referral.

held by a public sector agency, to which there is a right of access, is always available free of charge, whereas a reasonable charge may be made for information about a third party.

This approach, first instituted under the OIA and the LGOIMA, arguably has influenced the definition of what constitutes "personal information", so that the concept has been interpreted liberally to ensure that individuals enjoy the full measure of their legal rights. Thus, "personal information" has been interpreted to include comparisons of the requester with the successful job applicant for a position both had applied for;[27] the identity of informers in relation to the person being informed upon;[28] the identity of complainants;[29] and the identity of a requester's assailants.[30]

Limited direct access to courts

Under the OIA, LGOIMA and the Privacy Act (where the holder of the information is a public sector agency), requesters of personal information may enforce their rights directly in a Court of law, by-passing the specialist review procedures.[31] Direct recourse to the Courts was carried over from the OIA and LGOIMA to the Privacy Act on the grounds that this preserved exiting legal rights, the principle being "that a right once conferred by statute should not lightly be taken away."[32] This right was not extended in respect to personal information held by private sector agencies, however, as it was thought to be more cost effective to leave enforcement in the hands of a public official specialising in information privacy.

Although people (both natural and corporate) have a legal right of direct access to the Courts where their personal information is held by public sector agencies, they normally take the alternative route of pursuing their rights through the specialised processes provided under the OIA, LGOIMA, or Privacy Act. The principal reason for this seems to be that the review processes of the Ombudsman or Privacy Commissioner are undertaken without charge, and, in relation to the Privacy Act, there are no filing or hearing fees in the Human Rights Review Tribunal. Accordingly, recourse directly to Courts of law tends not to be made, despite a lengthy queue before the Privacy Commissioner is able to investigate a matter.[33] As was remarked in relation to practice under the freedom of information legislation prior to the Privacy Act:

---

27 Ombudsman's *Case No 737* (1987) 7 CCNO 59 (J Robertson); see also *Case Nos 194, 202,* and *226* (1985) 6 CCNO 111 (G R Laking); and *Case No 794* (1987) 8 CCNO 66 (J Robertson).

28 Ombudsman's *Case No 327* (1985) 6 CCNO 127, (G R Laking); *Case No 210* (1985) 6 CCNO 115, at pp 118 - 119 (G R Laking); *Case Nos 010W, 011W, 030W,* and *075W* of the Privacy Commissioner's casenotes (April 1994); *Hadfield v Police* (1996) 3 HRNZ 115; *Adams v New Zealand Police*, unreported, Decision No 16/97, CRT 3/97; *Cornelius v Commissioner of Police* [1998] 3 NZLR 373.

29 *Report of the Ombudsmen for the year ended 30 June 1997* (AJHR A.3) 35 - 36; (1997) 3(2) *Ombudsmen Quarterly Review* (June). This case was handled under the LGOIMA because the person requesting information about itself was a corporate, as opposed to a natural, person, and the information was held by the local council.

30 *Proceedings Commissioner v Commissioner of Police*, unreported, Complaints Review Tribunal, Decision No 18/2000, CRT 10/00, 10 July 2000.

31 THE HUMAN RIGHTS REVIEW TRIBUNAL IS NOT A "COURT OF LAW".

32 Report of the Department of Justice on the Privacy of Information Bill (22 January 1993) to the Privacy of Information Bill Sub-Committee of the Justice and Law Reform Committee, p 13.

33 In his report to Parliament for the year ended 30 June 2001, the Privacy Commissioner notes that the time between receipt of a complaint and its being assigned to an investigating officer dropped on average from 18 months to about 12 months).

> *The Courts, like the Ritz Hotel, may be open to all but only a few can afford the rooms. It is not surprising that no individual requester of personal information has taken the matter to Court.*[34]

Remedies

Under the OIA and LGOIMA, the remedy is simply a recommendation that the information concerned be disclosed in one form or another. The Ombudsmen's recommendations, even when they do not automatically convert into public duties, are normally adopted because of the great esteem in which the office of Ombudsman is held. No compensation or other remedies are available under the Ombudsman's review processes. Under the Privacy Act regime, however, compensatory damages are available as a remedy.

The majority of Tribunal cases where breaches of access rights have been found under the Privacy Act concern public sector agencies that would have been covered under the official information regime prior to 1993. Therefore, requesters under the Privacy Act regime now have available to them a remedy in damages which was unavailable under the official information regime.

A requester who has been denied access to personal information will have the evidential burden of proving whether or not there should be a remedy in damages, as well as the issue of quantum. It might be thought that cases involving breaches of access rights would be unlikely to give rise to compensatable loss, but this has not proved to be the case. Indeed, several cases have attracted substantial awards.

Nominal damages were awarded in two cases brought against the police. The amounts awarded were $500[35] and $200.[36] In one case, the police professed to have been unable to find the originals of several documents. The complainant was urgently seeking these for use in a private prosecution against a constable for failing to answer a summons served on him in the original hearing of several criminal charges against her. On the day of the hearing of her private prosecution, however, some of the documents sought were produced in evidence by the constable. Nominal damages were awarded on the basis that the evidence had no impact on the outcome of the hearing, and the original of the document she particularly sought was identical to a copy she had already seen. In the other case, the police refused to disclose the identities and addresses of the complainant's assailants on the ground that the request was frivolous or vexatious. The complainant was otherwise known to the police for having lodged a number of complaints and requests for information over the years, often in relation to matters in which he was not personally involved. The Tribunal found that the complainant suffered humiliation, loss of dignity and injury to feelings.

The highest award ever awarded by the Tribunal in an access case was $20,000 for humiliation, loss of dignity, and injury to feelings.[37] The complainant had supervised disabled children for the defendant organisation. He was suspended because a complaint had been made concerning an indecent assault by him on a child in his care. The complainant, however, had never been informed of the reason for his suspension nor was

---

34 I Eagles, M Taggart, and G Liddell, *Freedom of Information in New Zealand* (Auckland, 1992), 572-573.

35 *Mitchell v Police Commissioner* [1995] NZAR 274; [1995] 1 HRNZ 403.

36 *Proceedings Commissioner v Commissioner of Police*, unreported, Complaints Review Tribunal, Decision No 18/2000, CRT 10/00, 10 July 2000.

37 *L v N* (1997) 3 HRNZ 721.

he aware that the complaint had been taken to the police. He made a number of requests for his personal information, but was never given full information behind an internal inquiry into the matter, his suspension, or the complaint to the police. The Tribunal found that "the defendant embarked on a course of conduct which exacerbated the effect of the failure to confirm the existence of the information sought by the plaintiff." Among aspects of the defendant's conduct that were criticised by the Tribunal were the deliberate concealment of highly sensitive personal information from the plaintiff, even though it was obvious to the plaintiff at the time that this information was being made available to others; the defendant's concealment of the fact that it had destroyed the plaintiff's file and reconstructed another after the request for information had been made; the fact that the defendant had similarly misled the Privacy Commissioner during his investigation; and the obstacles which the defendant forced the plaintiff to overcome in his quest for his personal information, which caused an increasing number of people to learn of the damaging but unanswered allegation against him.

In another case, the High Court, on an appeal from the Tribunal, awarded $2,000 to a complainant because several documents had been withheld from him in the course of protracted employment litigation, apparently as the result of an oversight.[38] The Court found that the information would have been useful to the complainant's case. At the very least, the complainant would have been able to feel that he had presented his best possible case. The Court also accepted that the complainant "would have felt 'ambushed' and stressed" in the original hearing of his employment case when he became aware of the information that had been withheld from him, and he would have suffered further stress and disadvantage in having to decide whether or not to apply to have the newly acquired evidence introduced on appeal, where the respondent was contesting its introduction. The Court therefore awarded damages for injury to the complainant's feelings both at the time that he discovered that the information existed, and on an on-going basis. The Court commented that the damages award would have been higher had the complainant not delayed nearly a year in applying to have the new evidence admitted on appeal.

In a case against the Department of Child Youth and Family Services,[39] the Tribunal awarded damages of $2,500 because the Department had failed to make information available to the plaintiff in a timely fashion. The plaintiff had requested the information in connection with legal action he was undertaking against the Department for abuse while he was in its care as a child. The Tribunal accepted that the Department's treatment of a second request for information by the complainant caused him some humiliation. The defendant's staff had wrongly assumed that the plaintiff had already received the information concerned. The defendant's staff did not realise how important obtaining the information was for the complainant, and their conduct led him to believe that there was a conspiracy to withhold the information. The Tribunal, however, accepted the Department's explanation that there had been a series of errors and administrative changes that contributed to the problem. In another case against the same Department that also concerned a failure to grant timely access to personal information, the Tribunal awarded damages of $7,000 for humiliation, loss of dignity and injury to feelings.[40] The complainant, a secondary school teacher who taught students with special needs, had

---

38 *Proceedings Commissioner v Health Waikato Limited* (2000) 6 HRNZ 274.

39 *S v Department of Child Youth and Family Services*, unreported, Complaints Review Tribunal, Decision No 12/2000, CRT 13/00, 30 June 2000.

40 *DAS v Department of Child, Youth and Family Services*, unreported, Complaints Review Tribunal, Decision No 24/00, CRT 26/00, 13 September 2000.

been accused by a pupil of sexual abuse, and there was undue delay by the Department in disclosing the information relating to the allegation.

PRIVACY AND FREEDOM OF INFORMATION LEGISLATION IN NSW

Chris Puplick
New South Wales
Privacy Commissioner

New South Wales was the first State in Australia to pass a comprehensive State personal data privacy law, in the form of the *Privacy and Personal Information Protection Act* 1998. (PPIPA). Its core is a series of Information Protection Principles (IPPs). It applies the Principles by law to the public sector. It created the office of the Privacy Commissioner.

Under PPIPA, government agencies are required to have privacy management plans. If they wish, they can seek to have the application of one or more of the IPPs to their operations varied and adopt a Code of Practice, which must be drawn up in consultation with the Privacy Commissioner.

The interaction of the access and amendment rights given by PPIPA with those found under the *Freedom of Information Act 1989* (FOI Act) are addressed by clear provisions in PPIPA indicating that the relevant Principles do not override the FOI Act.

The FOI Act has both a privacy objective and a "democratic" objective, encompassing goals of participation, open government and accountability.

The FOI Act does not claim to exclude other means of obtaining access to information. Access to personal information may best achieved through the more informal and flexible arrangements mandated under PPIPA, but the FOI Act may continue to be the preferred way of dealing with more complex applications where, for example, there is an issue of disclosure of third party or confidential information or mixed personal and non-personal information.

PPIPA and the FOI Act have significantly different enforcement and review provisions. These and other important points of difference are noted in the following table.

Purpose	
FOI Act	To promote "openness, accountability and responsibility" in all public areas and to confer a legal right to access personal information and documents and to request amendments to records of a personal nature that are inaccurate, incomplete, misleading or out of date.
PPIPA	To promote fairness and accuracy in the way that personal information is collected, stored, used, accessed and disclosed and to govern the disclosure of personal information from "public registers".
Applies to	
FOI Act	Personal or non-personal information held by NSW government authorities, government ministers, local councils and other public agencies.
PPIPA	Personal Information about the individual held by NSW public sector agencies, including local councils and prescribed bodies which are outsourcing data services and personal information in public registers.
Modified by	
FOI Act	NA

PPIPA	Privacy codes of practice may modify, in relation to an agency or class of agencies, the operation of both the IPPs and the public register privacy principles. This includes exemptions from the operation of an IPP, as well as specifying the manner in which the IPP will apply.
Information covered	
FOI Act	Documents containing personal and non personal information including audio-visual film, tapes and discs.
PPIPA	Personal information including genetic material, electronic records, video recordings, photographs and biometric information.
Exempt Agencies	
FOI Act	Exemptions include some or all of the functions of some agencies including: Office of Auditor General; Director of Public Prosecutions; Independent Commission against Corruption; Public Trustee; State Bank of NSW; State Authority Superannuation Board; State Superannuation Investment and Management Corporation; NSW Ombudsman
PPIPA	State-owned corporations; Police Service; Independent Commission Against Corruption; Police Integrity Commission; Crime Commission, (except in relation to their administrative and educative functions)
Exempt Information	
FOI Act	NSW government cabinet and executive council documents (excepting those that are factual or statistical and do not disclose deliberations or decisions); documents exempt under Commonwealth or other States' FOI legislation; documents concerning law enforcement and public safety; subject to legal professional privilege; subject to secrecy provisions in other legislation; affecting the: personal affairs or business affairs of another person or business and the economy of NSW. Additionally, documents may be subject to a Ministerial Certificate stating that a specific document is exempt and restricted.
PPIPA	Information in publicly available publications and information or an opinion about a person's suitability for appointment or employment as a public sector official. Several of the Information Privacy Principles are also declared to be inapplicable if the agency is lawfully authorised or required not to comply with the principle concerned, or if non-compliance is otherwise permitted (or is necessarily implied or reasonably contemplated) under an Act or any other law.
Exempt Functions	
FOI Act	Judicial functions of courts and tribunals and the investment, complaint handling, investigative and reporting functions of certain agencies.
PPIPA	Some exemptions apply to the law enforcement, investigative and complaints handling activities of certain agencies.
Applicant/Complainant	
FOI Act	An individual or group of individuals or a corporation or Association
PPIPA	An individual. Third party complaints may not be allowed
Application or complaints procedure	
FOI Act	Application in writing to the agency for access to specified documents held by the agency. The agency must advise in writing within 21 days that the information is available, or if the request has been deferred or refused. This period may be extended by a further 14 days if special circumstances apply, such as the need to consult with a third party. Application fees: A$30 Processing fees A$30 an hour. Requests for an internal review to be made in writing within 28 days of being told of the agency's decision. Review application fee: A$40

PPIPA	Complaints about alleged breaches of privacy or applications for access to personal information, preferably in writing, can be made to the agency or the Privacy Commissioner. The agency is obliged to inform an applicant whether they hold personal information about the applicant and give access to it without undue delay or expense. Under Pt 5, the individual may seek an internal review of the agency's conduct or decisions regarding an alleged breach of the IPPs, a code of practice, or the public register provisions in Pt 6, or they may make a complaint to the Privacy Commissioner under Pt 4. If the individual complains under Pt 5, the agency must then conduct an internal review and notify the Privacy Commissioner, and it may request the Commissioner to undertake the internal review on the agency's behalf. If the individual makes a complaint to the Commissioner Under Pt 4, the Commissioner must attempt to resolve the complaint by conciliation, and, on completion of an investigation, can only make reports and recommendations.
Review	
FOI Act	If dissatisfied with the internal review, the applicant may request that the NSW Ombudsman investigate. The Ombudsman can make recommendations but cannot change or reverse a decision. Or they may request that the Administrative Decisions Tribunal (ADT) review the agency's decision. The ADT can make a fresh determination. The ADT can be used either as an alternative to an external review by the Ombudsman or after the Ombudsman has completed an external review.
PPIPA	Under Pt 5, if the person is dissatisfied by the internal review, or the action taken by the agency as a result, or if the review is not completed within 60 days the individual can make an application to the Administrative Decisions Tribunal for a review of the conduct concerned.
Remedies	
FOI Act	The ADT can recommend that it is in the public interest to give access to a document which has been refused as exempt; the decision of an agency be reconsidered; action be taken to change the agency's conduct; reasons be given for a decision; or the law or practice be changed.
PPIPA	Any application to the ADT may go to the findings of the agency review or to the action proposed to be taken by the agency. The Tribunal may decide not to take any action following review. If it considers that action is warranted it may make one or more of the following orders: monetary compensation up to $40,000; restraining order; specific performance order; correction order; remedial steps order; non-disclosure order in the case of public register complaints; and ancillary orders.
Overlap	
	Agencies can refuse notification, access or correction rights under sections 13 to 15 of the Privacy and Personal Information Protection Act by using an exemption available to that agency under the FOI Act

THE RELEVANT JURISDICTION OF NEW SOUTH WALES ADMINISTRATIVE DECISIONS TRIBUNAL

Judge Kevin O'Connor
President, Administrative Decisions Tribunal
New South Wales[1]

In the State of New South Wales in Australia the Administrative Decisions Tribunal is the external body in which unresolved disputes arising under the State's *Freedom of Information Act 1989* (FOIA) and *Privacy and Personal Information Protection Act 1998* (PPIPA) may be determined.

The Tribunal follows procedures broadly similar to those of a Court. The Tribunal's orders are final and binding. These disputes are heard in the General Division of the Tribunal before a single member of the Tribunal, known as a 'judicial member'. The term 'judicial' is used to distinguish legally qualified presiding members from members from a non-legal background, the latter being known as 'non-judicial members'. A judicial member needs to be legally qualified. Typically the member is a practising barrister or solicitor who sits at the Tribunal on a sessional or part-time basis. The Act setting up the Tribunal, the *Administrative Decisions Tribunal Act 1997* (ADTA), requires that the President be a Judge of the District Court of the State. (This is the main trial court of the State, an intermediate court in the judicial hierarchy, responsible for hearing most serious criminal charges and most personal injury claims as well as commercial disputes up to $A750,000).

An appeal from a decision of the General Division of the Tribunal may be made to a three member Appeal Panel of the Tribunal. The Appeal Panel is usually presided over by the head of the relevant Division; or the President. The second member must be a judicial member of the Tribunal, and the third must be a non-judicial member. The Act permits an appeal to made on a 'question of law' with an appeal in relation to disputed findings of fact only being permitted by leave of the Appeal Panel. In practice the Appeal Panel has required that an error in the legal reasoning of the Division before shown before it will consider re-examining the findings of fact. A further appeal is available from the Appeal Panel to the Supreme Court. The appeal may only be made on the basis that there is an error in the legal reasoning.

*****

FOIA provides citizens with a right of access to documents held by public sector agencies. An agency is broadly defined and includes any body set up by statute, which includes for example all Universities in New South Wales and covers local government councils. Some government bodies have exclusions from the operation of the Act.

Most FOI cases in the Tribunal relate to the question of whether an agency was entitled to refuse access to documents because the documents are protected by a category of exemption set down in the Act (for example, in-confidence communications, Cabinet documents, personal affairs of third parties, law enforcement documents). Typically the exemption categories are formulated in a multi-factored way and it is necessary for the agency to demonstrate to the satisfaction of the Tribunal that each of the requirements of the exemption is met in the circumstances before its decision will be upheld.

---

1 Formerly Federal Privacy Commissioner, Australia 1989-1996.

Citizens also have a right to apply for amendment of documents to which they have been granted access which relate to their personal affairs. The Tribunal has now dealt on a number of occasions with questions such as the approach to be adopted in assessing whether it should order that an opinion be amended, as distinct from merely permitting the applicant to have a notation of his or her view added to the record.

FOI proceedings in the General Division take the form of an 'application for review' of the agency's decision. Typically an applicant's access or amendment application will have been the subject of an initial decision by the agency, and an internal review by the agency before it comes to the Tribunal. It is also possible for an applicant after the internal review stage to make a complaint to the Ombudsman in relation to the agency's decision. The Ombudsman has investigative staff and relevant powers. In light of the investigation, the Ombudsman may chose to intercede on behalf of the citizen and make recommendations to the agency, for example, to release more documents or make amendments. The agency is not bound by these recommendations but usually accepts them. Though not required to do so, citizens often go to the Ombudsman first and then bring their case to the Tribunal. The Tribunal does not have any investigative staff of its own though it has relevant powers, so it is substantially reliant on the applicant and the parties for evidence and submissions.

The Tribunal's order-making powers in relation to FOI matters are set out in the ADTA and are to affirm, vary or set aside the decision; or to remit to the agency with recommendations.

These are the powers typically given to tribunals in Australia that are responsible for undertaking 'merits review' of administrative decisions by Ministers, agencies and officers of agencies.

PPIPA lays down information protection principles to be observed by public sector agencies. Like the FOI Act, these are widely defined. If a citizen considers that the conduct of an agency contravenes an applicable information protection principle or an applicable code of practice or involves disclosure of personal information kept in a public register, the citizen may apply to the public sector agency for a 'review of the conduct'. The public sector agency is required to notified the State Privacy Commissioner on any such complaint. The Privacy Commissioner may make submissions to the agency internal review, and may, at the request of the agency, undertake the internal review on behalf of the agency. If the citizen is not satisfied with the outcome of the internal review, he or she may apply 'for a review of the conduct that was the subject of the application [to the agency]'.

In contrast to the position in FOI cases, the Tribunal has a wide power to make appropriate orders in PPIPA cases. In may require the payment of monetary compensation in respect of a contravention to a maximum amount of $A40,000. It may for example require an agency to cease contravening conduct, to engage in conduct consistent with the principles or to correct personal information that has been disclosed.

The information protection principles of the PIPPA became binding on public sector agencies on 1 July 2000. The Tribunal's jurisdiction commenced on the same date, subject to its power to make a monetary compensation order being deferred for a further 12 months until 1 July 2001.

There are presently several applications under the PPIPA at the preliminary stages in the Tribunal, but so far there has been no case in which a hearing has been held on the

question of whether conduct constitutes a contravention of an information protection principle.

The information protection principles are set out in Part 2 of the Act, and follow the familiar sequence of limitations on collection of personal information, requirements in relation to methods of collection and the scope of collection, principles as to retention and security of information, information as to the existence of systems and practices, rights of access and alteration, principles as to data quality, limitations on the use of information, limitations on disclosure of personal information and special restrictions of disclosure of sensitive categories of personal information. The Act creates an office of Privacy Commissioner, and that office is responsible for implementing the legislation. It has wide power to conduct inquiries and investigations. Complaints may be made to the Privacy Commissioner of 'alleged violation of, or interference with, the privacy of an individual'. This is a broad jurisdiction and goes beyond a complaint as to conduct of the kind that can be dealt with (also) by the Tribunal. The Privacy Commissioner is obliged to seek to resolve complaints by conciliation. The Privacy Commissioner, like the Ombudsman in FOI matters, may make recommendations to a respondent to a privacy complaint as to what action might be taken in response to the complaint.

*****

When an application for review of an agency decision under the FOI Act or an application for review of conduct by an agency under the PPIPA is made to the Tribunal, the Tribunal initially lists the application for, what is called, a 'planning meeting'. This is a preliminary hearing where a judicial member canvasses with the parties the question of the extent to which the dispute remains capable of resolution without going to hearing. Often the issues in dispute are reduced at this stage. Sometimes a new compromise is reached, and the proceedings discontinued. The Tribunal has the power to appoint mediators, to give the parties an independent, neutral evaluation of the dispute and to commission an assessor to make findings of fact on matters requiring special expertise. So far it has not been found necessary to use any of those special powers in either FOI or PPIPA cases.

In most cases the Tribunal gives detailed written reasons for decision. Our decisions in relation to FOI and PPIPA cases can be located using the search engine on the Caselaw NSW web-site. This site can be reached via the ADT web-site, which is www.lawlink.nsw.gov.au/adt or directly at www.lawlink.nsw.gov.au/caselaw/caselaw.nsf/pages/adt.

******

Finally, I should note that FOIA and PIPPA are two of approximately 100 State statutes that confer jurisdiction on the Tribunal. The Tribunal has three broad areas of responsibility – merits review of government administrative decisions (including occupational licensing decisions); civil determinations relating to equal opportunity complaints and retail leases claims; professional discipline inquiries (lawyers, veterinary surgeons).

PUBLIC REGISTER PROVISIONS – ADDRESSING PRIVACY ISSUES

Blair Stewart
Assistant Commissioner
Office of the Privacy Commissioner, New Zealand

> *The many statutes that require, permit, or prohibit the disclosure of specific categories of public records would appear to offer a wealth of material from which more general principles can be deduced and policies can be isolated. In practice, this is much more difficult than it appears. For many statutes it is not possible to find materials explaining why the law was written in a particular way. Even if materials may be found, they may not reflect current controversies.*
> - Robert Gellman, *Public Records, Access, Privacy and Public Policy*, 1995

> *You may be aware of this Council's prolonged challenge regarding the ability of organisations to access personal information from the building consent register. The outcome favoured releasing the information. It is frustrating, therefore, that such an outcome would seem to totally contravene the spirit of the Privacy Act. Irrespective of the prevailing legislation, this Council firmly believed that more weight should have been given to the purpose of collection of the information and its commercial value. Suffice to say, that along with probably every other local authority in New Zealand we are now selling on a cost recovery basis, building consent information to organisations which intrude upon the privacy of individuals to use it for commercial gain.*
> - Dunedin City Council in a submission on the Privacy Commissioner's review of the operation of the Privacy Act

There is one species of freedom of information law which predates the Official Information Act, and allowing for the release of public information even in the era of the Official Secrets Act 1951. This is the public register law.

Character of public registers

Public register provisions are sections in statutes (less usually regulations) which establish registers of information open to public search. Registers are essentially formal records set down in a systematic way for use and retrieval (sometimes they go by other names such as databases). Registers of information are quite structured compared with the vast range and forms by which information is held by public bodies. The legal right of access to public registers is derived from the laws which establish the registers themselves not more the general Official Information Act rights.

The Privacy Commissioner has contrasted public register access rights and Official Information Act access rights as follows:

> *Obtaining information from a register pursuant to a statutory search right differs in nature from an Official Information Act request. In an Official Information Act request, the register sets the parameters through the scope of the request. A register search, on the other hand, does not usually have this individualised quality. Requests for information from a register must fit the requirements of the agency maintaining the register and not the other way round. A request under the Official Information Act requires an official to consider whether there are grounds for withholding the information. Judgment and discretion are called for, and occasionally consultation. The official may withhold information although before doing so will consider any countervailing public interest favouring disclosure. A*

> *request for information from a public register is far more mechanistic. If the Registrar's requirements are met, such as through the use of a search form or the payment of a fee, the information in standardised form will be released, usually quite promptly. The Official Information Act does not derogate from provisions in enactments which authorise or require official information to be made available. Statutory search rights concerning registers are such provisions.*[1]

Public registers throw up a host of privacy issues. The Privacy Act, and initiatives by the Privacy Commissioner, have highlighted the issues (and in some cases resolved them) but much work needs to be done to satisfactorily reconcile the privacy and competing public interests. (At present, the issues are not reconciled, the privacy interest is merely disregarded under most public register laws.)

Public register issues and risks

Public registers have particular characteristics which carry special privacy risks and raise difficulties in legally and practically addressing those risks in an effective fashion.

In considering the privacy risks one should bear in mind the following characteristics of a typical public register:

- information on the register will be logically arranged to enhance use and retrieval – while this is essential to the proper functioning of the register for its necessary purposes, it also makes it an especially attractive source of information for other purposes
- only key authoritative information is registered – unlike many other record systems (such as government files), a statutory register is unlikely to be cluttered with extraneous materials such as draft documents or correspondence, making it straightforward to locate relevant and reliable information
- the register will have a degree of institutional permanence – enabling third parties to plan elaborate and on-going processing of the data for unrelated purposes
- individuals will be compelled by law to supply personal information for the register or else they will commit an offence or be unable to undertake some activity
- certain sets of information exist only in public registers since individuals are unwilling to provide the information voluntarily
- a statutory right to search the register exists which restricts a Registrar's discretion to withhold information.[2]

Accordingly, many public registers are attractive propositions for all sorts of third parties who would wish to use them to obtain information about individuals – indeed, some businesses repeatedly "mine" public registers and sell the results. Briefly stated, the central privacy issues with public registers revolve around the fact that individuals have no choice but to supply their details which may then be published and will be given out on request to whoever wishes to have the information without regard to purpose for which the information will used or the harm that any such use may cause an individual.

Typical public register problems are:

- their use for tracing individuals for reasons unconnected with the purpose for which the register was established, whether those reasons be relatively benign (preparing a

---

1 Privacy Commissioner, *Necessary and Desirable: Privacy Act 1993 Review*, 1998, footnote 8 to para 7.2.8.

2 This list of the characteristics of a typical public register is taken from Privacy Commissioner, *op cit*, para 7.1.7.

family history) or malign (tracking an estranged partner who has fled from an abusive relationship)
- bulk retrieval of personal information on public registers by commercial interests which use and sell the information for direct marking purposes or for profiling individuals (for instance, as to their wealth or creditworthiness).

The Privacy Act attempts to deal with some of the public register privacy issues. One way that it does this is by establishing a set of four public register privacy principles touching upon:
- search references
- use of information from public registers
- electronic transmission of personal information from public registers
- charging for access to public registers.[3]

Unfortunately, the public register privacy principles do not provide a complete or effective solution to public register privacy issues.[4] The Privacy Commissioner has recommended a scheme of amendments to the Privacy Act which would turn the public register privacy principles into a far more coherent and effective response to the problems. However, statutory amendments to give effect to those recommendations have not yet been made. Therefore the balance of this paper is directed to the approach of the public register provisions themselves, that is the laws which establish public registers and provide the legal authority for public access to those registers.[5]

When legislation creating a public register is contemplated or being reviewed the information privacy implications need to be considered. This note discusses how legislative provisions might be drafted to resolve privacy problems. Careful attention must also be given to accompanying administrative or technical controls which are not discussed in this note.

Establishing public registers

A first issue is whether to establish the register as a "public register" for the purposes of the Privacy Act. Establishing the register as a "public register" by listing the statutory provision in the Second Schedule of the Privacy Act as a "public register provision" means that the public register privacy principles, and other aspects of Part 7 of the Privacy Act, will apply. However, it also means that the "publicly available publication" exceptions to the information privacy principles come into play.

A further consequence is that it will mean that it is possible for Part 6 of the Domestic Violence Act to be applied to the register. However, the application of that Act is dependent upon further regulations being issued and therefore there is an opportunity to explore, as an entirely separate issue, whether that information suppression regime is appropriate for the register.

---

3 See Privacy Act 1993, s.59.

4 For a fuller account of why the principles are not effective see Privacy Commissioner, *op cit*, chapter VII and Blair Stewart, "Five Strategies for Addressing Public Register Privacy Problems", 21st International Conference on Privacy and Personal Data Protection, 1999, 87.

5 The material that follows is an edited and updated version of a note entitled "Drafting Suggestions for Departments Preparing Public Register Provisions" which was released as guidance for officials in December 1999.

Generally a register established by law, carrying with it a specific public search right, should be created as a "public register". The relevant provision(s) should be added to the Second Schedule of the Privacy Act by statutory amendment or pursuant to an Order in Council issued under s.65 of the Privacy Act.

Any proposal to create or continue a statutory register, and to provide a statutory right to search, needs careful consideration from a privacy perspective. The drafting approach makes a considerable difference to whether privacy problems are created or solved. The older approach of establishing a public register by merely stating that certain documents or information are to appear on a public register and be open to public search, leads to a host of privacy problems. A bald statutory provision like that makes reconciling the collection and disclosure of personal information with the information privacy principles difficult or impossible. However, a number of new legislative provisions over the last few years demonstrate innovative drafting techniques and legal controls that may resolve the privacy concerns.

There are 7 features in a modern public register provision that the Privacy Commissioner looks for in seeking to resolve privacy concerns. Not all would need to be present in any particular case. They are:

(a) statements of purposes (for the register and for the public search right)
(b) a list of the permitted search references
(c) limitation on the register content available for search
(d) a right to search on a "need to know" basis
(e) a restriction on the bulk provision of information from the register
(f) provision for suppression of certain personal details in exceptional cases
(g) a control on the use of information obtained from the register.

(a) *Statement of purposes*

It is desirable to identify the purposes for any new public register and to state these in legislation. This is a first step to reconciling the operation of the register with the reasonable expectations of Parliament and citizens.

It should be noted there are often two ways in which "purpose" is spoken of in this context. The first is the purpose for establishing the register. The second is the purpose for giving a right to search to people other than officials. In some cases it may be unnecessary to provide both explanations. Sometimes, the purpose for public search will be obvious from the context, or can be derived from the other statement of purpose. Surprisingly, this is not always the case and there are cases where officials maintaining registers are perplexed at the reason why Parliament ever created a right for third parties to search the register.

Recent examples where laws set out the purpose of a public register in a transparent manner can be found in:

- Local Government Act 1974, s.122ZI(1)
- Animal Products Act 1999, ss. 18, 52, 73 and 112.

Examples setting out of the purpose of the right of public search can be found in:

- Local Government Act 1974, s.122ZI(1)
- Personal Property Securities Act 1999, s.173.

(b) *Appropriate search references*

One of the key privacy safeguards in the public register privacy principles relates to "search references". Public register privacy principle 1, for instance, requires that personal information be made available from a public register only by search references that are consistent with the manner in which the register is indexed or organised.

To obtain information from a public register a searcher will normally quote a search reference. Search references are essentially required for ease of administration. Registrars will logically order their records which were originally stored in filing cabinets consistent with that ordering. Search references naturally flowed from the subject matter of the register or from the way it was organised.

These mechanisms ensure protection of privacy in a pragmatic, although imperfect, way. Someone who can quote the reference might be thought to have some sort of business seeing the relevant information held.

Settling upon the appropriate search references is an important part of the task of addressing public register privacy issues. It requires consideration of what search references are believed to be appropriate to achieve the purposes of a new register and, for example, whether searches by name should be required or prohibited.

The issue becomes extremely important as we are now in an era of "e-government" in which registers will often exist only in a computer database. Since the physical constraints of filing systems will not protect privacy, the legal and administrative constraints have heightened importance.

Examples of statutes which expressly set out search references include:

- Local Government Act 1974, s.122ZI(5)
- Radiocommunications Act 1989, s.28(2)
- Personal Property Securities Act 1999, s.172.

It is desirable that search references be specified in the legislation itself.[6]

(c) *Content of register available to search*

What personal information should be on a register? How much of that should be made publicly available? These are key questions when determining the risks to privacy and how they may be addressed. The content should be set out in the legislation. The information necessary for behind- the-scenes administrative use does not necessarily all need to be made publicly available. This needs to be carefully considered on the basis of what is necessary for the purposes for which the register is set up, and for the right of public search, as well as any risks to privacy.

---

[6] It is sometimes appropriate to allow for further search references to be added by delegated legislation. For example, under s.122ZI(5)(c) of the Local Government Act further search references can be added by regulations under the Local Government Act or by a code of practice under the Privacy Act. If legislation establishing a new public register also sets out its purposes, this can guide the process of evaluating consistency of new search references with the register's primary purpose.

Examples of legislation which lists the contents of a register and specifies a subset available for public search include:

- Dog Control Act 1996, ss.34 and 35
- Land Transport Act 1998, s.199.

Residential address is a significant detail that may carry particular privacy risks if released. Several approaches have been tried to address this issue (see also suppression schemes at (f) below).

Address details are not, for instance, released from the register of driver licences or for the rolls used for school trustee elections.[7] Such details are available from the dog register in only limited cases.

It has been proposed for some future legislation that *full* address will not always have released to the public. Instead release could be limited to a person's suburb or town.[8]

Section 28(3)(a) of the Radiocommunications Act 1989 provides that residential address information of natural persons may not be released if the individual concerned has notified the Registrar that he or she does not allow this (an "opt-out" arrangement).

(d) ***Search rights on "need to know" basis***

Most privacy concerns do not arise from the use of the registers for the primary purposes for which they were established. For the most part, the privacy concerns about open public registers relate to use for *other* purposes. Sometimes these purposes are directly or indirectly related to the primary purpose. Sometimes they have nothing to do with it. On occasion secondary uses are actually incompatible with the primary purpose (eg. where they discourage registration).

Accordingly, one of the best ways to reconcile privacy interests with privacy concerns, is to establish a regime whereby information is channeled from the register to people who have a proper "need to know" the information so that it will be used for purposes compatible with the register. This approach brings the operation of a public register closer to the approach of the information privacy principles.

At the end of the day, this approach means that the statutory register will not have the full, open and unrestricted nature of most older existing public registers. However, for users with an appropriate need for the information, registers will remain open and accessible.

An example of a public register which was reconstituted on this basis is the dogs register, open to search under s.35 of the Dog Control Act 1996. Briefly, the way that that register operates is that it is:

- open on an unrestricted basis to a list of designated officials and bodies; but
- otherwise information identifying a dog owner's address is only released to the general public on a search for certain approved purposes.

The permissible purposes are set out in the Act. A mechanism is provided so as to ensure the public searches are for the specified purposes, requiring members of the

---

7 Education (School Trustee Elections) Regulations 2000, reg. 6(3).

8 This has been proposed for electoral and motor vehicle registers.

public to identify themselves and to declare what their search is for. Search forms have been issued by regulation.

When specifying classes of persons who may search a register, this may be the place to set out access by government officials as well (although this is not strictly a public access matter). An example of specifying classes of persons, including officials, who may search a register is to be found in:

- Dog Control Act 1996, s.35
- Personal Property Securities Act 1999, s.173.

Further, s.199 of the Land Transport Act 1998 differentiates between information on the register for official purposes and that available for public search.

(e) *Bulk provision of information*

A notable privacy problem for some registers is requests from businesses for details of many or all entries on a register for commercial use outside the purposes of the register. A typical such secondary use is for direct marketing.

An example of an attempt to address this problem by restricting bulk provision of information from a public register can be found in the Rating Valuations Act 1998, s.52(f). This provides that regulations may be made prescribing limitations or prohibitions on the bulk provision of district valuation roll information for purposes outside the purposes of the Act.

(f) *Suppression of personal details in exceptional cases*

The best approach from a privacy perspective is to establish a new public register with a clearly stated purpose, with search references consistent with that purpose, and for access to be given to appropriate content on a "need to know basis". However, sometimes there really will be a need for an absolutely unrestricted search right, and therefore one may need to consider safeguards which fall below this ideal. One approach is to recognise that certain people have particular needs to have some of their details suppressed. The common example is of residential address.

The need for, and workability of, such proposals depends upon which information is intended to be publicly displayed on the register. If the register is intended to also include residential address then some consideration should be given to allowing individuals to establish a case on certain grounds to have their address, or the entry, suppressed or held on a confidential register.

Examples of suppression mechanisms include:

- Transport (Vehicle and Driver Registration and Licensing) Act 1986, s.19(5)
- Radiocommunications Act 1989, s.28(3)
- Electoral Act 1993 s.115
- Domestic Violence Act 1995, Part 6
- Fisheries Act 1996, ss. 102(3), 129(3).

The ground usually specified for a suppression provision is the personal safety of the person or his or her family. Sometimes other interests such as a fear of harassment, desire to preserve privacy, or national security, may be specified.

Residential address is not the only sensitive detail. Section 27(3) of the Building Act 1991, for instance, controls access to any plan or specification that has been marked as being confidential because of, among other reasons, the requirements of the owner relating to the security of the building.

The confidential register provisions are a useful backstop even if a privacy-friendly regime, as described above, is established. It may be that reasonable privacy expectations can be met through options (a) to (e), but that people having special concerns for their safety still need something extra to guarantee their personal well-being. However, confidential register provisions alone are no substitute for the privacy approach mentioned in (a) to (e).

(g) *Use of information obtained from a register*

The techniques mentioned earlier are directed towards specifying the content of a register, establishing the purposes of public search, and setting controls on who might be able to access personal information on the register. As an alternative to establishing the register on a "need to know basis" (or as a supplement) it is possible to devise a regime which would place special controls on the subsequent use of information so obtained ensuring that information obtained from the register is not misused in a particular way.

This approach has not been widely adopted in New Zealand. However, it is a mechanism which can work well with a general free flow of information in most cases. The creation of a control such as this will link with the articulated purpose for which a register is established.

An example where this technique has been utilised overseas is s.216J of the Corporations Law of Australia which states:

> **Use of information from registers**
> (1) A person must not:
> (a) use information about a person obtained from a register kept under this Part to contact or send material to the person; or
> (b) to disclose information of that kind knowing that the information is likely to be used to contact or send material to the person;
> unless the use or disclosure of the information is:
> (c) relevant to the holding of the shares, options or debentures concerned or the exercise of the rights attaching to them; or
> (d) approved by the Company.
> (2) A person who contravenes subsection (1) is liable to compensate anyone who suffers loss or damage because of the contravention.
> (3) A person who makes a profit from a contravention of subsection (1) owes a debt to the Company. The amount of the debt is the amount of profit.

In New Zealand, s.116 Electoral Act 1993 provides that certain people who have access to information from the electoral roll on computer tapes commit an offence if the information is used for a purpose other than one authorised in the Act. Similarly, s.200 of the Land Transport Act 1998 limits the purposes for which officials may use photographic images from the Driver Licence Register. These are both examples of controls on use by specially approved classes of agency having privileged access to register information not generally publicly available.

The Stasi Files:

How a special access regime balances openness and privacy in relation to secret police files

Dr. Alexander Dix, LL.M.
Commissioner for Data Protection
and Access to Information
Brandenburg

Statement at the
International Symposium
on Freedom of Information and Privacy
Auckland, 28 March 2002

Overview/Contents

- **Short history of the German Stasi Records Act**
- **Main provisions**
- **Cause celèbre: Helmut Kohl**
- **Where do we go from here ?**

The Ministry for State Security

- Ministerium für Staatssicherheit (col. abbreviation in the GDR: *"Stasi")*
- In 1989 the MfS had 91 000 official staff and 174 000 unofficial collaborators ("IMs")
- Thus the ratio was 1 spy for every 62 inhabitants of the GDR - an intensity of surveillance probably unparalleled worldwide.

Landesbeauftragter für den Datenschutz und für das Recht auf AkteneinsichtLandesbeauftragter für den Datenschutz und für das Recht auf Akteneinsicht Brandenburg

Short history of the Stasi Records Act (1)

- Stasi Records Act 1992 - a major achievement of the East German civil rights movement
- The Treaty of Unification had to be amended after civil rights activists took possession of the Stasi Files *(„Where is my file ?")*
- For the first time in history the files of a secret police (of a dissolved state) were opened for inspection. This turned out to be a *conditio sine qua non* of German unification.

Landesbeauftragter für den Datenschutz und für das Recht auf AkteneinsichtLandesbeauftragter für den Datenschutz und für das Recht auf Akteneinsicht Brandenburg

Short history of the Stasi Records Act (2)

- The West Germans considered the Stasi files an issue which the East Germans as main targets of surveillance should decide upon themselves
- The Stasi Records Act was adopted by the Parliament of the unified German Federal Republic on the basis of an Act passed previously by the first (and last) freely elected Parliament of the German Democratic Republic

Landesbeauftragter für den Datenschutz und für das Recht auf AkteneinsichtLandesbeauftragter für den Datenschutz und für das Recht auf Akteneinsicht Brandenburg

The main issue: Openness vs. Privacy (1)

- "We are visiting a political and legal territory beyond the framework of our constitution in order to pay even greater respect to the rule of law in our present republic." *(Joachim Gauck)*
- The task was to reconcile the aim of bringing the documented results of an oppressive regime out into the open with the principles of privacy protection.

Landesbeauftragter für den Datenschutz und für das Recht auf AkteneinsichtLandesbeauftragter für den Datenschutz und für das Recht auf Akteneinsicht Brandenburg

The main issue: Openness vs. Privacy (2)

- Under German Data Protection Laws the Stasi files (as results of illegal spying on people's private lives and intimate relationships) arguably should have been destroyed
- On the other hand the dignity of the victims called for them to be given the right to see their files and to find out who spied on neighbours or even spouses

Landesbeauftragter für den Datenschutz und für das Recht auf AkteneinsichtLandesbeauftragter für den Datenschutz und für das Recht auf Akteneinsicht Brandenburg

The main issue: Openness vs. Privacy (3)

- Inspecting one's own file has been called the "Magna Charta" of privacy protection
- But the Act also allows for the use of the Stasi files for historical research and media publication in order to understand the functioning of the Ministry for State Security ("No future without past")

Landesbeauftragter für den Datenschutz und für das Recht auf AkteneinsichtLandesbeauftragter für den Datenschutz und für das Recht auf Akteneinsicht Brandenburg

Main provisions (1)

- Right of data subjects (victims) to inspect their own file and to have informers named
- Right of other data subjects to inspect their files (as long as legitimate interests of victims are not touched upon)

Landesbeauftragter für den Datenschutz und für das Recht auf AkteneinsichtLandesbeauftragter für den Datenschutz und für das Recht auf Akteneinsicht Brandenburg

Contentious Anonymisation

Data subjects (victims and other person concerned, not informers) may apply for anonymisation or destruction of their files as from 1 January 2003 if

- there is no overriding interest of other data subjects who would otherwise suffer a lack of evidence,
- the personalised files are not needed for historical and political research

Landesbeauftragter für den Datenschutz und für das Recht auf AkteneinsichtLandesbeauftragter für den Datenschutz und für das Recht auf Akteneinsicht Brandenburg

Main provisions (2)

- A Federal Agency (Commissioner for the Stasi Records) collects and administers the files and processes applications for inspection
- Public bodies employing or considering employment of staff and private companies for their chief executives may ask the Federal Commissioner for information about possible collaboration with the Stasi (until 2007)

Landesbeauftragter für den Datenschutz und für das Recht auf AkteneinsichtLandesbeauftragter für den Datenschutz und für das Recht auf Akteneinsicht Brandenburg

Main provisions (3)

- For the purpose of research related to the political and historical reappraisal of the functioning of the State Security Service researchers and the media may access
  - records with no personal data,
  - records with personal data of persons of contemporary history, political office holders and public officials while in office, *unless they are data subjects or third parties*
  - records with personal data on employees or beneficiaries of the State Security Service

Landesbeauftragter für den Datenschutz und für das Recht auf AkteneinsichtLandesbeauftragter für den Datenschutz und für das Recht auf Akteneinsicht Brandenburg

Cause celèbre: Helmut Kohl

- Former Chancellor Kohl (who had been subject of Stasi surveillance while in office and who had signed the Records Act himself) sued the Commissioner to prevent him from opening to researchers and journalists personal records which the Stasi had kept
- Kohl's success before the courts led to a discussion about the future of the Stasi Records

Some figures

- 123 km of records in the archives of the Federal Commissioner
- 16 km shredded material still waiting for reconstruction
- More than 1,7 Mio. data subjects have seen their records 1992-2001
- More than 1,5 Mio. applications by public employers to screen their staff were handled

Where do we go from here ?

- The Stasi Records will eventually become part of the Federal Archives
- They will always remain special due to the circumstances of their collection
- The Stasi Records Act has had followers in Central and Eastern Europe
- The question is: why should the Secret Service of a democratic state not be made public sometimes in the future ?

Links

- http://www.bstu.de/englisch/index.htm
- http://www.lda.brandenburg.de
- http://www.privacy.de =http://www.datenschutz-berlin.de

A Researcher's View Of New Zealand's Official Information Act

Nicky Hager
Wellington, New Zealand

During the 20 years since New Zealand's Official Information Act (OIA) came into force I have made many hundreds of official information requests, covering a wide range of subjects and state organisations. I also have experience of seeking official information in other countries. I would like to share some of these experiences with you.

I will begin by noting the good things about the Official Information Act. First, although our act is not as strong in various way as the US Freedom of Information Act (FOIA), it has the important advantage that you can request more than just specific existing documents. Under our act you request "information", not documents: answers to questions, lists of data and so on, whether or not they are contained in a document. Another great strength is that our act is based on the "principle of availability", where all information must be released by agencies unless there is an expressly stated exclusion clause which applies to the specific piece of information requested.

The reason why I have used the act so often is that I find it a powerful tool that allows access to a lot of important information. However, my experience has been that the act also has major limitations.

The purpose of the Official Information Act, as stated in section 4, is *"to increase progressively the availability of official information to the people of New Zealand"* – that is, the intention was that over time information would become more available. Despite 20 years of operation, there has not been a review to investigate whether the act is fulfilling this purpose. My experience is that it is not. While there has undoubtedly been an increase in the total *volume* of information sloshing around, I think there has been a reduction in the *availability* of important information that affects people's lives.

For a while in the 1980s, after the act was passed, I found there was a genuine shift in public service attitudes towards freedom of information. Staff were well trained for Official Information Act work and, mostly, there was a developing culture of openness. The approach of the Labour Government in the late 1980s changed that, and throughout the 1990s there was increasingly closed government. Ministers and officials developed ways of routinely subverting the provisions of the Official Information Act, including delaying information releases and misusing exclusion clauses. My suspicion is that many users of the Act give up before getting their information, and maybe never try again, as it often takes months fighting through the Ombudsman to obtain information that should have been released immediately. I thought things might improve with the election of the current government in 1999, but my personal experience is that there has been little improvement and in some areas it has got worse.

I will run through a list of the ways that I find myself regularly held up or blocked when requesting information – a list that adds up to a sort of "how to" guide for unhelpful government officials. I will conclude that we are long overdue for a review of freedom of information in New Zealand and so, as I go through the list, I will note the areas where legislative and other changes are needed.

1. Time limits for responses

The Official Information Act states that departments and Ministers should reply 'as soon as reasonably practicable, and in any case not later than 20 working days' [after receipt of a request]. Most departments and Ministers have unilaterally chosen to interpret this as meaning they are not required to reply before 20 working days (the maximum time has become the minimum), even sitting on the reply until the deadline. The majority of my requests take more than 20 working days and often much more. You can complain to the Ombudsman, but that usually takes longer than the delays anyway. Officials have learned they can get away with delays, without sanction, so they are untroubled by time limits. This alone means that for requesters such as deadline-conscious daily journalists the Act is often useless. In a future review of the OIA, there need to be shorter time limits and significant sanctions on agencies and Ministers that do not make reasonable efforts to meet them. Agencies respond to written parliamentary questions in five working days, so I suggest that 10 working days (with the possibility of extensions) is appropriate for OIA requests.

2. The need to have the Ombudsman's intervention

At least half of the time, when the response at last arrives, you find that some or all of the information has been refused – and frequently the parts you want most. This means that, in addition to the delays to date, there is no option but to complain to the Ombudsman and wait up to several months longer while the officials' decisions are investigated and reviewed. Thus the effective time for responses becomes more like 50-100 working days, and sometimes longer. Some requests take years. I have no doubt that quite often refusals are intended deliberately to delay or put off requesters. The tactical value of stalling for months to avoid public scrutiny is obvious. The issue may well be decided and over, old news, by the time you get your information. The answer here is tightening up the time limits, removing unwarranted exclusion clauses, providing more resources to the Ombudsman's and Privacy Commissioner's offices and introducing sanctions that hurt for non-compliance with the act.

3. Unhelpful officials

My experience is that, once the Ombudsman has reviewed the officials' decisions, I almost always get considerably more information than I did in the initial response. Literally, for over 90% of complaints. Consider what this means. It means that, at least with my requests, officials are – regularly and routinely – being more considerably more restrictive with official information than they should be if they followed the act properly. It should not be necessary to complain to the Ombudsman to get information.

There are two possible reasons for this restrictiveness. The first is the growth of information controllers in government and state agencies: professional "communications" or PR people whose job it is to manage and restrict the information that reaches the public. There is plenty of scope for deliberate bending of Official Information Act requirements for tactical political reasons. Sometimes it is blatant. I recently waited seven months through an Ombudsman's investigation to get some information from the Ministry of Economic Development (I had initially had a blanket refusal). Yet two weeks before the Minister, Paul Swain, released the information to me, he had his staff drop a bundle of the key papers I had requested to every parliamentary journalist. Why? This is a trick used by Beehive staff to stop the requester, who has done the work of obtaining the information, from being able to write an exclusive story. After waiting seven months and then being scooped by the Press Gallery, there was no point in

using the information I finally received. The Ombudsman should be able to impose sanctions for uncooperative and obstructive behaviour.

4. Lack of training of OIA staff

The other possible reason for restrictiveness is lack of understanding of the act. The 1981 Danks Committee Report, which provided the basis for the Official Information Act, argued sensibly that no law would work unless there was co-operation from the agencies; in other words, a culture of freedom of information. In the first years of the OIA there was an Information Authority that actively trained departmental OIA staff. This training was effective at enhancing the culture and practice of freedom of information. Today there is no such training and my impression is that many officials do not understand the act. It often looks as though the officials decide what they would rather not release and then idly thumb through the act looking for a few clauses to cite in justification. These decisions frequently do not stand up to Ombudsman review. The Ombudsman regularly calls for more OIA training. The creation of an equivalent of the former Information Authority would help a lot.

5. Exclusion clauses

Although the OIA is based on the principle of availability – and "increas[ing] progressively the availability" – I have found that the exclusion clauses are being used increasingly to reduce the availability of information. Partly this is deliberate and accidental misinterpretation of the clauses, but also some clauses drafted 20 years ago have turned out to be increasingly restrictive in ways I doubt the drafters anticipated. There are three areas where this trend is most striking.

5.1 COMMERCIAL SENSITIVITY: When the OIA was drafted in the early 1980s, no one could have foreseen how much official information would one day be excluded under the commercial and economic exclusion clauses (6(e) and 9(2)(b)). State-owned enterprises, hospitals, universities, foreign affairs, the environment ministry... you name it, all of these public organisations now claim that large areas of their work is protected from public scrutiny by commercial considerations. If the purposes of the OIA are to be fulfilled into the future – that is, that there is increasing availability of information to allow public participation in decisionmaking and effective government accountability – then these clauses need to be rewritten to give priority to democratic necessities.

5.2 INTERNATIONAL AND SECURITY ISSUES: Likewise, in this era of international agreements on trade and other matters, access to information on these issues is of highest priority. However, section 6(a) and (b) exclusions have grown to be major obstacles to freedom of information, allowing "international relations" secrecy to speed to cover all manner of domestic issues too.

One of my areas of research has been intelligence agencies. In New Zealand, the wording of the OIA is so weighted in favour of secrecy for intelligence agencies that they are, in all important ways, excluded from the Act. The book I wrote on electronic intelligence agencies and their operations contained, on nearly every page, very secret details of these agencies gained from interviews with intelligence staff. I believe that the release of much of the secret information had high public interest value. It showed politicians being misled by officials, international spying operations that had been kept secret from the government and operations that were at odds with stated foreign policies. However, much of this information was classified as Top Secret and higher than Top Secret, which means, supposedly, that its release would cause damage to New Zealand security and

intelligence operations - not "adverse" or "significant" or "serious" damage, but "*exceptionally grave*" damage. The book came out and has been translated into other languages and reported around the world. It probably embarrassed the agencies concerned, but - as generally is the case with these big secrets - the sky did not fall down and there was in fact no "exceptionally grave" damage or even much damage at all. Intelligence agencies - perhaps like all agencies - have certain legitimate areas where their activities need, at least for a time, to be secret. But the balance needs to be shifted much more in the direction of accountability. The same goes for foreign policy and defence. Otherwise, the only practical option for democratic accountability is going around the laws and obtaining leaked information.

5.3 SECRECY OF GOVERNMENT DECISION-MAKING: The other growth area of government secrecy is the section 9(f) and (g) exclusions. These two often misused clauses allow for information to be withheld to enable "free and frank expression of opinions" between Ministers and officials and to "maintain constitutional conventions" with respect to advice given to Ministers. Ombudsman's decisions have repeatedly confirmed that neither of these clauses should be interpreted as meaning that all official advice and other documentation may be withheld, but the clauses are nevertheless used over and over to discourage and stall requesters. The first purpose of the Official Information Act is "*to enable more effective participation in the making and administration of laws and policies*". Obviously that means being able to have the necessary information to participate *before* the decisions are made. The current government repeatedly interprets these clauses as allowing all information on decision-making (including sometimes even that decisions are being considered) to be withheld until after the Cabinet has made its decisions. By that time it is often a bit late to try to participate in the making of the laws and policies.

In each of these areas, and a few others, there is a need for changes to the 20-year old Official Information Act to shift the balance considerably in favour of freedom of information. If anything, information laws should err on the side of openness, not secrecy.

6. Charging as a means of discouraging requests

When all else fails, officials sometimes use their discretionary power to impose charges for the time it will supposedly take to locate and collate the requested information. Often the proposed charges are absurdly high (many thousands of dollars). However in my experience - as I said, hundreds of requests - I have only ever paid one charge for information. Most departments do not ask for them, Ministers generally never do and so, in my experience, charges are usually only requested where the officials are trying to be particularly unhelpful. In most cases of charging, I have had the charges overturned by an Ombudsman's review. However, charges do serve as a potential means of at least stalling the requester.

Clearly, government agencies cannot be expected repeatedly to divert their staff for weeks to someone's OIA requests. What would be desirable here is an equivalent of the US FOIA waivers for public interest requesters (journalists, public interest groups etc) while charges remained an option for other requests.

7. Bad record-keeping inhibiting freedom of information.

Each year there is a greater and greater volume of official information but record-keeping capabilities and archiving techniques are not keeping up. In the 1982 world, when the

OIA was introduced, most information was on paper. Now it is mostly not on paper, which makes freedom of information much harder (for instance, with interdepartmental drafts circulating and never being filed as hard copies).

Also, in 1982 there were clerical staff whose job it was to file everything in an orderly way and there was a stricter culture of putting things on the file. In contrast, today much of the business is conducted via short e-mails, a lot of it of little consequence, with inadequate guidelines as to which bits need to be filed. The lack of organised files makes access much harder (and withholding, losing and hiding files easier).

In one recent case, I requested correspondence and minutes of meetings between a Crown Research Institute (CRI) and an industry lobby group over a two year period. The CRI replied that the only way it could fulfill my request was to search through all the computer tapes containing e-mail backups, requiring 96 person days of work which would cost me $20,000. On top of this would be another $20,000 for the cost of leasing computer equipment for the task. And that wasn't all. The director of the CRI explained that the e-mails had encryption protection, so it would take a further 2,800 days of chargeable time to make the backups readable. In total, over ten years work and a million dollars of charges! From an archive perspective, they almost may as well throw away the tapes now. There is apparently an urgent need for a review of government policies and instructions on record keeping.

8. A review of freedom of information in New Zealand.

My conclusion is that New Zealand is overdue for a thorough review of the freedom of information laws (including the OIA, Local Government Official Information and Meetings Act and other legislation). The terms of reference should clearly state that the point of the review is to improve freedom of information, otherwise there is a risk that the review could be used by people in the government system whose preference is to restrict information. As mentioned, it should cover time limits for responses, the exclusion clauses, official obstructiveness, official record keeping, charging, training, Ombudsman and Privacy Office resources and the creation of a freedom of information training and monitoring organisation.

A good option would be for the official information laws to be reviewed as part of a wider review of freedom of information; allowing progress on related issues such as access to parliamentary information, routine electronic access to government information (without the requirement for OIA requests) and access to public interest information held by private organisations (as in the South African laws). For example, the Australian government website has a search engine allowing searches, without charge, of all parliamentary questions and Hansard transcripts. In New Zealand a private company controls electronic access to this basic public information and you must pay to search it. An independent review process for responses to written parliamentary and select committee questions is also needed. In "e-government", I think the objective should be that, for instance, unclassified cabinet papers and government decisions will be made available on-line routinely within, say, one week of the decisions.

I want to thank the Privacy Commission for taking the initiative and organising this event. I feel that there has been complacency in New Zealand over the decline of freedom of information. This is a good time for changing that. It will need all the people concerned about freedom of information - many of whom are here - to advocate actively for strengthening the laws and providing the resources needed to implement them.

TAKING FREEDOM OF INFORMATION LAWS INTO THE FUTURE

Blair Stewart
Assistant Commissioner
Office of the Privacy Commissioner, New Zealand

Freedom of information laws are stuck in a time warp. Whether enacted in the 70s, 80s, or 90s, many FOI laws still maintain 1970s thinking. They hark back to an era of 'Big Government' and rudimentary information technology. They draw on ideas which were radical in their time but which now do not go nearly far enough.

I intended those words to be a somewhat provocative introduction to a presentation to a 1999 conference in Hong Kong.[1] In fact, the conference was disrupted by a typhoon.[2] I am therefore pleased, at last, to have the opportunity offer suggestions for freedom of information (FOI) law into the future.

Since the enactment of the Official Information Act 1982 (OIA) there have been vast technological advances in collating, duplicating and disseminating information. There has also been a sea change in public administration. Government departments have transformed themselves into new and unfamiliar legal structures. Parts have been hived off into trading enterprises, outsourced or privatised. Change has been replicated at local government and public utility level. FOI laws have been caught up in these changes but the results have not always been beneficial. Frequently the entities that carried out public services have been exempted from FOI laws when privatised or corporatised.[3]

No discussion of information handling would be complete without contemplating the effects of the Internet. We stand at a threshold (or portal?) through which can be seen grand plans for "joined-up-government". Whether one is excited or disturbed at the prospect of e-government, there will be consequences for traditional FOI. This may be the time to enhance citizens' rights – after all can a month's wait for access under the OIA or Privacy Act be squared with thousands of officials having the same information at their fingertips in milliseconds? Notwithstanding the Internet's obvious potential for freeing the flow of information, few FOI laws have directly addressed any issues arising from it. While the OIA is usually seen as virtuous in being media neutral – focusing on information rather than documents – is it being bypassed in the modern age?

I offer 8 suggestions. The ideas take into account public sector reform, automation of information systems and today's emphasis on international standards and human rights. I ignore the many familiar problems under which existing FOI laws, including the OIA, labour (e.g. lack of resources to promptly handle requests or review refusals). These must also be addressed.

---

1 Freedom Forum Asian Centre & Library and Privacy International Seminar on "Freedom of Information: The People's Right to Know", Hong Kong, 16 September 1999.

2 Recently notes of my proposed remarks were published as "Taking Freedom of Information Laws into the 21st Century", 6/1 *Human Rights Law and Practice* (July 2001) 55.

3 While privatised bodies cease to be covered by the OIA, New Zealand legislators – in contrast to many overseas – have tended to keep state-owned enterprises within the coverage of the OIA. This pro-FOI approach has recently been reaffirmed and extended to Local Authority Trading Enterprises: see Local Government (Elected Member Remuneration and Trading Enterprises) Amendment Bill 2001.

Review and renew

1. *Every FOI law should include a requirement, and mechanism, for regular review.*

   One often hears complaint that FOI laws are not working as effectively as they ought. Glaring shortcomings often remain unremedied. Even minor fine tuning is put off.[4]

   As well as reviewing machinery provisions, existing exemptions for agencies and information should be reassessed periodically. For instance, should the legislature and its committees be outside the coverage of FOI law?[5]

Comprehensive coverage

2. *The application of FOI laws should be broad and of continuing relevance.*

   Every new public body established, formally or informally, should be covered by an FOI law unless there is good reason to exempt it.[6] Any decision to exempt must be taken in a transparent and publicly accountable way, subject to periodic review. There should be a presumption of comprehensive coverage.

3. *Bodies carrying out significant public functions should be subject to FOI requirements whether they are structured as private or public bodies.*

   Given public sector reforms, this is essential if FOI is to remain a reality in important parts of citizens' lives.[7] Private sector bodies should be subject to FOI law only in respect of their carrying out of public functions.

---

4 As part of the Privacy Commissioner's review of the operation of the Privacy Act I obtained, and studied, legislative review reports from a number of overseas jurisdictions particularly within Australia and Canada. Some excellent recommendations for reform of information access laws were made, many of which were simple fine tuning. Almost without exception, no action has been taken on such reports. The Commissioner's own report made 25 recommendations concerning "good reasons for refusing access to personal information" and "procedural provisions relating to access and correction of personal information": see Privacy Commissioner, *Necessary and Desirable: Privacy Act 1993 Review*. That report was given to the Minister of Justice in November 1998 and like the Law Commission's report, *Review of the Official Information Act 1982*, October 1997, it remains unimplemented.

5 Grant Liddell has made a case that Parliamentary institutions should be subject to FOI laws: Grant Liddell, "The Official Information Act 1982 and the Legislature: A Proposal" in Legal Research Foundation, *The Official Information Act*, February 1997. The Privacy Commissioner has also proposed enhancing personal access rights as they relate to Parliamentary institutions: see Report by the Privacy Commissioner to the Minister of Justice in relation to the Parliamentary Service Bill, November 1999.

6 New Zealand Cabinet Office processes do ensure that this issue is expressly considered every time a public body is established by statute (although there are some inconsistencies in the decisions actually taken). The process does not require periodic review of any decision to exempt a body from the OIA.

7 This is, I believe, a critical challenge. It may be possible to confer access rights in particular areas where there are particular public interest needs. This approach has been taken in Europe with the development of information rights specific to the environmental area where the public may have an equal need to know about the pollution practices of a private business as with a state-owned one.

4. *Individuals should have access to personal information held about them by private sector bodies as well as all public bodies.*

This has been the law in New Zealand since 1993, pursuant to the Privacy Act, and has recently become the law in Australia. A number of European data protection laws accord access rights to corporate bodies in respect of personal data relating to those bodies. Perhaps there might be a case to extend the personal rights of access possessed by corporate bodies under Part IV of the OIA into the private sector as well?

Routine disclosure, active dissemination

5. *FOI laws should oblige agencies to routinely disclose and actively disseminate information of public interest.*

FOI laws which solely focus upon request and response will never fully achieve open government. RD/AD emphasises identifying possible public interest in a document (before ever receiving a request) and consequently circulating information about the document, or the document itself, to those likely to be interested.[8] There are many other steps that can be taken such as having an easily distributed "public edition" with excisions (if needed) and putting frequently requested documents in real or electronic reading rooms.

6. *Enhancements in information technology must be harnessed to achieve the objectives of FOI laws.*

Many FOI laws can cope with the existence of electronic data merely through the application of existing provisions and there is a case for FOI laws to remain technology and media neutral. However, the Internet offers opportunities for *enhancing* freedom of information not merely simply adapting FOI laws. In particular, it is now possible to signal the existence, and make directly available, both routine and obscure documentation through sophisticated use of websites and electronic mailing lists.

Global transparency

7. *FOI should be enhanced and supported at international level.*

Access to information has been a feature in several remarkable transitions. South Africa had its Truth and Reconciliation Commission, an exercise in revealing official information and personal experience, in exorcising apartheid. Something similar is planned for East Timor. Germany opened the Stasi files. Access law in Hungary, Poland and the Czech Republic is an important feature of these renewed democracies. Glasnost in the USSR was a key feature in its transition to the rule of law. The role of FOI laws in modern democracies should be included in international human rights discourse as a mechanism to promote government transparency and to counter corruption. Perhaps FOI should be included as conditions in World Bank or IMF restructuring packages? Is an international FOI treaty warranted?

---

[8] See, for example, Information and Privacy Commissioner/Ontario and Management Board Secretariat (Ontario), *Routine Disclosure/Active Dissemination (RD/AD),* April 1994.

Transparency should apply to international and supranational institutions themselves. As a starting point, individuals should have access to, and correction of, personal information held by such institutions about them. While a veil of secrecy has traditionally existed in relation to international institutions there are promising moves. Interpol has a data protection supervisory committee which oversees personal access and rectification entitlements.[9] The European Union has made significant moves in the areas of personal access[10] and general FOI.[11] While transparency at international level has intrinsic merit there is a flow-on in terms of openness at national level. Typically FOI laws provide a blanket reason for withholding information which is received from a foreign government or an international institution. That traditional approach should be reviewed.

Rights, remedies, enforcement

8. *Rights are not sufficient on their own, the public must be assisted to effectively utilise FOI laws.*

Citizens should not need a lawyer to exercise FOI rights. Easy-to-use processes, with the minimum formality and cost, are essential. Information commissioners, or access ombudsmen, are highly suitable mechanisms. Tribunals and courts are best reserved for exceptional cases or for appeals. The public must also be well informed of their rights and officials trained in their obligations.

Many reasonably successful FOI laws rely upon Ombudsmen-type mechanisms. However, even with well respected institutions and generally compliant civil servants, anyone with a passing knowledge of FOI practice knows that there are ministers, civil servants and particular public bodies, who regularly flout FOI laws. Compensation is a valuable and central feature of the personal access regime under the Privacy Act.[12] Thought could be given to extending compensation to unjustified refusals to give personal access to corporate bodies – at the very least, where an unjustified refusal causes harm or detriment.[13] While it would be a significant policy departure to allow for damages in general OIA cases, and might conceivably lead to an undesirable litigious-minded approach, might exemplary damages be an appropriate sanction in extreme cases? Should criminal sanctions exist for ministers or chief executives who instruct their officials to breach the OIA?

A number of information access rights exist which provide no easy route to obtain review of a refusal short of taking proceedings in the High Court.[14] High Court proceedings, while valuable, do not provide a readily accessible, cheap or appropriate means of review for most citizens. Might the compliance processes established

---

9 The 1998 Annual Report of the Supervisory Board for the Control of Interpol's Archives reports, for example, 21 requests, for access, deletion etc.

10 The EU Data Protection Directive is to be applied to community institutions with an EU Data Protection Commissioner to provide oversight and independent review.

11 See the recently adopted EC Regulation 1049/2001 on Public Access to Documents held in Community Institutions.

12 Privacy Act 1993, s.66(2).

13 Those personal access rights are found in the Official Information Act, Part IV, which unlike the Privacy Act carries no rights to compensation. "Refusal" also encompasses undue delay in actioning a request.

14 For example enabling shareholders to obtain access to certain company documents.

under general FOI and privacy laws be suitable for adaptation to these other statutory rights?[15]

[15] This is already sometimes done. For instance, the Privacy Commissioner is the review authority for refusal of information requests made under the Health Act 1956, s.22F.